FOURTH SECURITY SEALS SYMPOSIUM
TAMPER-INDICATING DEVICES
June 15-16, 1999
Oxnard, California

Naval Facilities Engineering Service Center
Security Engineering Division (Code ESC-66)
1100 23rd Avenue
Port Hueneme, CA 93043-4370

CONTENTS

CONTENTS (cont)

FOURTH SECURITY SEALS SYMPOSIUM
TAMPER-INDICATING DEVICES
June 15-16, 1999
Oxnard, California

OPENING REMARKS –

Eric Elkins, Symposium Chairman and Technical Manager, Department of Defense (DoD) Lock Program, Naval Facilities Engineering Service Center (NFESC)

Good morning. I would like to welcome everyone to the Fourth Security Seals Symposium. I work at the Naval Facilities Engineering Service Center (NFESC), some of you know us from our previous name as Naval Civil Engineering Laboratory. Like other military organizations we have consolidated, moved, and changed our name. My job is the Technical Manager for the DoD Lock Program. I manage the DoD Lock Program because of DoD Directive 3224.3, which assigns various aspects of physical security development and procurement to the various services. The Navy's responsibility is for the locks, safes, vaults, seals, and containers program. We are the Lock Program Team and we are happy to host this symposium. We are hosting our fourth symposium because of the number of requests and positive responses from the people in the community. The objective of this symposium is to provide technology transfer. We have worked real hard to put together an agenda that will provide valuable information. To help make this symposium truly successful, we need to get as much participation from you, the attendees, as possible. Please bring up issues you wish us to address and we will work hard to get to those issues. If there is anything our team can do while you are here, please let me know. The Project Manager for the Seals Program is Jeff Miller.

At this point I would like to introduce our Commanding Officer, CAPT Westberg, Jr.

WELCOME ADDRESS –

CAPT Robert J. Westberg, Jr., Commanding Officer, NFESC

Thank you. Good morning and welcome to Port Hueneme. A lot of you are from the East Coast so welcome to the Fourth Security Seals Symposium. I have learned a lot of what these folks are doing, what you are doing, and what industry is doing in this vital area of security for the nation and the DoD. I think this is a tremendous program, and the Engineering Service Center (ESC) is really proud of its role and its participation.

I have only been at the ESC for a couple of months and I am still in the process of personally moving up here. So I have kind of personal idea of how important it is to know where and how your valuables are stored. Keeping track of your stuff is a hard thing and I wish I had known about the Radio Frequency Identification Device (RFID) technology of tracking. I would liked to have tagged everything we own. But this drives home the point of how important tagging is, knowing where your things are, and having them secure. As technology improves the things we need in order to conduct military operations or take care of the programs that you are involved in and as the products become more valuable, the importance of keeping track of them

and having security grows. This industry and the work you do are becoming more vital. Military operations succeed or fail based on logistics. It is important to know where your things are and being able to get to them when you need them to conduct operations. The technology like the RFID and others enable us to know whether something has been tampered with and this is vital for military operations. I encourage you to take advantage of the time here with the experts. Learn as much as you can. If you are a user, provide all the needs you have to the experts so they can continue to refine and make the technology better. Again, I welcome you and I hope you enjoy the next few days.

Eric Elkins: I have the pleasure this morning of introducing our Keynote Speaker. I have been asked not to go into a lengthy bio and I thank him for that because he has a very lengthy bio. I will tell you he is the Director of Security in the Office of the Deputy Assistant Secretary of Defense, C3I Command, Control, Communications, and Intelligence. He is the highest ranking civilian in the Department of Defense in the area of security. He started as a Navy Officer, Naval Material Command, moved to Defense Investigative Security Command, and now works in the Pentagon and has held a number of offices. He has a lot of information to give us and is highly recommended by the people who have heard him speak in the past.

KEYNOTE ADDRESS –

Richard F. Williams, Director of Security in the Office of the Deputy Assistant Secretary of Defense (Security and Information Operations), Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) – Concurrently Deputy Director of the DoD Special Access Programs Coordination Office

IT WAS REQUESTED THAT PORTIONS OF THIS PRESENTATION NOT BE RECORDED.

The key stone elements of security:

- Personal security
- Information security
- Physical security - Cost the most, most people don't want to spend the money. It is however, very effective.
    - Psychological barriers – There is a new brainwave machine out there that helps detect when a person lies. We know the brain is in direct line with the eye. A signal will be sent that helps detect lies and we can measure that brainwave. This is the psychological aspect.
    - Physical barriers – Guard at the door is a simple physical barrier.

SECURITY REQUIREMENTS

- Change in the way physical security has been addressed. That is lightening up. Spending too much money, we have less standards, less requirements. What we have seen is a fundamental change two or three times from where it goes heavy to light.

Locks, how much or how many is enough? When do they buy the physical barrier? After a break-in. That is usually when people look into security. The Department of Energy (DOE) is taking a leadership role, you need take action.

OBSERVATION

- Security professionals must be able to ride the waves of change. This is what I am challenging you to do. Get into the front, stay ahead, and come up with the right kinds of products. Products that we can really use, something we really need and put it to an application and make suggestions.

NATIONAL INDUSTRIAL SECURITY POLICY SHAPING REQUIREMENT FOR THE FUTURE

- New Assistant Secretary of Defense (ASD) (C3I) organization
- Potential threats of 125 countries - number one nuclear weapons, loss of nuclear material, chemical weapons, big issue is biological weapons. We are leaving information age, in the last 25 years 75 percent of what we know has been invented.
- Changing nature of the world – coalitions trying to take control.
- Pillars of security – differences of the way we do security. Computers have changed the way business is being handled.
- The new operating environment - everything with nothing. Get this back on track.
- Observations – real important not to count on upper personnel for the answers, you need to come up with the correct answers, drive the information up from the bottom.

STATUS REPORT, DoD SECURITY SEALS PROJECT -
Jeffrey Miller, Project Manager, DoD Lock Program Technical Office, NFESC

Good morning, thank you all for coming. I am the new Project Manager for the DoD Lock Project, but I am counting on Mike Farrar, Eric Elkins, and you for support with the security project.

SECURITY SEALS – GOALS

- Provide user guidance on availability or what type of seal will most effectively meet specific requirements
- DoD Training Course for Effective Seal Use
- Revise Federal specifications
- Establish and chair the Fifth Security Seal Symposium

SECURITY SEALS - ACCOMPLISHMENTS for FY99 – We have developed the following:

- Anti-Pilferage Seal User's Guide - This guide helps the user understand the role of the seal and when seals should be used. It also provides the user with insight into using

seals effectively with a good seal control program in selecting and installing seals for various applications. It is available in hard copy, CD-ROM and also on our web-site. Mike was pretty much in charge of this effort and we feel he did a great job.

- Developed DoD Training Course for Effective Seal Use – Mike and I worked closely with Dr. Roger Johnston from Los Alamos National Labs (LANL) in developing this course. This course provides the user with the seal history, guidance with how to install, remove, inspect, and maintain a seal control program. It is in the final review and should be completed soon.
- Our last major accomplishment has been the update of the seal spec FF-S-2738 – some of the major revisions included removing pressure sensitive seals, the electronic seals, and I believe the fiber optic seal from that spec. We also revised some of the testing requirements; presently this is being incorporated into the system and should be out any time now.

SECURITY SEALS - FUTURE

- Complete DoD training course for effective seal use.
- FY-2000 we are considering the development of a Federal or ASTM spec for Pressure Sensitive Seals, if this happens we will update the Seal User's Guide to include Pressure Sensitive Seals.
- We are considering adopting electronic seals for DoD and talk about the Fifth Symposium – this is an excellent arena for technology transfer.

Eric Elkins: Can you spend a little time on the essence of the spec that replaced the federal specification, how it works. More detail on selection and procurement of seals.

Jeff Miller: The topic is the advantage of the new FF-S-2738. Hopefully we can get more control on seals for what we use, and the testing program. The seals previously aren't really being tested to anything. Even though the old specification was there, seals weren't being bought and tested. We are trying to make sure that the seals meet these environmental tests (i.e., pull strength) so that the user can see and select what he needs for his various application.

Mike Farrar: The most important thing is the fact that this puts the testing on the government instead of the manufacturer. Some of the manufacturers have a hard time with this, but the only way the Government can be sure of what we are getting is to do the testing ourselves.

Question: I s this testing being carried out now?

Mike Farrar: No, the testing is not being carried out now. The seal's specification has been approved and will be published, hopefully, within the next 90 days. Some of the things that need to happen:

- The guidance documents need to require that seals being used meet the requirements of FF-S-2738. This has not happened in the past. If you don't have requirements, you are lost.

Question: Where is the testing being done?

Jeff Miller: There are a variety of tests in the specification, covert and surreptitious tests, environmental testing, it depends of the type of test and what needs to occur.

Bob Loughlin: What you are saying certainly implies that the American Society for Testing and Materials (ASTM) standards program has failed to meet the needs of the government. Where do you think ASTM fits into this program now and in the future?

Jeff Miller: We've looked at ASTM for these particular seals and we just thought we might loose some control over it if we adopted ASTM specifications at this point and time.

Mike Farrar: The specification refers to the ASTM standard for physical testing, as to the physical properties of the seal. But the ASTM doesn't address covert and surreptitious. This is one of our main concerns - covert and surreptitious. All the physical testing on FF-S-2738 refers to the ASTM standards, but the covert and surreptitious does not.

Bob Loughlin: ASTM is there to do this if the industry and users want to make it happen. It's a consensus program. Efforts to try and get it going are on the mind and should they be the ones participating?

Eric Elkins: I think this is something we should expand on Bob. I think we can take a look at that in the committee. To answer this gentleman's question about whom is going to do the testing? The procurement agencies, the people who are going to buy the seals, are the people who select the testing agency. What we have in the DoD is through the Defense Industrial Supply Center (DISC). They have had as many as 200 seals listed on their security seals listing. None of them have been tested. People wanted to have seals available through the supply system. Now if there were a requirement, as Mike said, to use a certain type of seal that has been tested against a specification, then the procurement agency is bound to buy a seal that, in fact, meets those requirements. What they (procurement agency) would do is put a solicitation out on the street asking companies to submit seals against this specification. If you are a manufacturer and you want to submit seals they will find a testing laboratory. Most likely they would ask our organization because we run the Lock Program for the DoD to do that. We will do some of the testing, or subcontract out some. What we want to do is test the best we can. So if they hire us to do it we will get the testing done. The seals that get approved will then be procured by DISC. The advantage of this over the system they are using now is that every manufacturer has the same opportunity to sell seals to the Government. The way it is now, hit or miss. Seals are just being evaluated. There is no set testing procedures that they go through. This would be a huge advantage to the manufacturers.

James Najar (ELC Security)**:** At past symposiums we have talked about a formal letter regarding the lead and wire seal usage by the DoD. Are these revisions going to be taking that into consideration, is that letter going to be forthcoming?

Jeff Miller: That letter was sent out 1 1/2 years ago.

James Najar: It hasn't gotten to the manufacturers.

Mike Farrar: That letter is out and directed to the users of DoD seals that they should not use and will not use lead.

Jeff Miller: In our Users' Guide we have shown some replacement possibilities.

Bruce Roberts (Encrypta)**:** In the last few months I have had several Government or DoD organizations that have called me asking about lead seals, and where they could obtain them. So your letter apparently is not as well read as you would think. One of them happens to be at Port Hueneme.

Tim Besse (CSSG/DoD)**:** Are there Federal specifications for other types of security seals?

Jeff Miller: In the old specification there was but not now. We have removed them and are looking to develop other specifications for DoD. For pressure sensitive seals, we are looking at that one, and we are considering electronic seals.

Tim Besse (CSSG/DoD)**:** So at this time there are no federal specs for optic locks or other electronic seals or RFID?

Jeff Miller: That is correct.

Richard Williams: I would like to see some seals. I would like to see:

- Some watermark seals on the back of XO7 locks.
- Computer cases - So that if anyone opens them you would be able to know.

There are a number of other things that we would be interested in that would serve or help in other areas of security. You would need to go a little farther than that if you want to make this a constructural barrier. This is something to be concerned about and I hope you got that out of my speech. We will put the requirements in.

THE SECOND OLDEST PROFESSION:
7000+ YEARS OF SEAL USE, PLUS AN
ATTEMPT TO PEER INTO THE FUTURE

Dr. Roger G. Johnston
Los Alamos National Laboratory
Los Alamos, NM

I for one, appreciate this symposium. I suspect there are some who would say that certain aspects of the seals business should be lumped in with the worlds oldest profession, and I'm not sure that is really fair. It is helpful to see where seals fit in historically and try to put them into historical context. It is clear that tamper detection has been important throughout human history and always will continue to be so.

We know for a fact that seals are at least 7,000+ years old. You can visit museums in Europe and see that there are massive displays of stamp seals. The earliest seals (we don't have examples) were made out of wood or bone. Some of the earlier seals:

- Stamp seals
- Carving stamp seals
- Press seal into clay, imprint
- Carving stamp seals, seal impressions.

The earliest seals were tokens made of stone, clay, or marks of teeth. You wanted to protect them, take the tokens and seal in the clay ball, stamp with seal, later these were used for trading. Later on, these would be used for legal contracts before writing was invented.

- Also used in pottery, the seal impression would show what the container was used for
- Loom weight – Designation would show the weight value

The stamp seal impressions were also used for both tagging and sealing purposes. When writing was invented it started out as clay tablets. You would do your impressions with a stick into a clay tablet. When you were done, you would stick your stamp seal impression into the clay representing a signature or author-dictation to prove you were the author of that clay table. That was the tag function.

Then, if you wanted to detect tampering you would stick that clay tablet into a clay envelop which also had writing and apply another seal impression. The idea was to detect tampering. If someone tried to read the clay tablet or tamper with the text, they would have to break open the envelop which would then destroy the seal impression pattern.

Earlier stamp seals were to put a pattern on a Bulla. Bulla is a chunk of clay that is elongated like a football. The way it would work, if you had a package you wanted to protect from tampering you would tie the package up with string and make a nice knot. Take a lump of clay (Bulla), stick it around the knot, and imprint your seal pattern onto the clay. In showing two views of broken Bulla from Syria before 3,000 BC, you could still see the impressions of the string and the knot on the inside.

Other ways people used stamp seals for tamper-detection – if you had objects you could roll up into mats, tie a rope around it, put clay there and then imprint your seal pattern into the clay.

The Egyptians had their own tamper-indicating devices based on baskets. What they would do is on the underside, inside the lid on a basket they had a loop of the wicker material. On the front of the basket they had a wooden dowel which had a hook on the inside. The dowel would either be pushed in or out ,or rotated or both. The hook would engage the loop on the inside of the lid. When they would seal the wicker basket, they would rotate the dial into position to grab the loop to prevent you from opening the lid, then use a piece of clay on the front and imprint their seal impressions. This made opening difficult and hard to replicate.

WHY DID CYLINDER SEALS BECOME SO POPULAR?

- Easy pattern replication
- Fun and cool
- Symbolic – Symbol of life
- More area available for art
- Could be worn on necklace – If you lost it you could report it, stand in the center of town, and have it announced. With that, if someone tried to use it everyone would know it was reported lost.
- Better impressions?
- Harder to counterfeit?

USES FOR ANCIENT SEALS – Continuing today

- Security of rooms
- Security of goods (in transit and storage)
- Security of documents
- Authenticity of documents
- Customs and taxation
- Trademarks
- Personalization
- Ceremony

USES FOR ANCIENT SEALS - Now mostly extinct

- Decoration
- Mark of ownership - before writing was invented
- Time and location stamp
- Signature and legal authority
- Royal seals (from 2,000 BC)
- Designations (e.g., loom weights)
- Religion, magic, and charges

MODERN SEALS

- Active –
  - electronic and fiber optic
- Passive –
  - wire loop seals
  - metal cable seals
  - plastic strap (ribbon) seals
  - metal ribbon (car-box/car-ball) seals
  - bolt seals
  - "padlock" seals
  - adhesive tapes and labels (pressure-sensitive)
  - passive fiber optic seals
  - secure containers
  - tamper-evident packaging
  - security clamps

WHY COMPLEX, HIGH-TECH SEALS WILL BE VULNERABLE TO SIMPLE ATTACKS

- Still must be physically coupled to the world
- Still depend on the loyalty and effectiveness of user's personnel
- More legs for an adversary to attack
- Users don't understand the device
- Developers have the wrong expertise
- Developers and users focus on the wrong issues
- The arrogance of high technology

PREDICTIONS

- More re-usable seals (electronic and electro-optic)
- More seal readers
- More wireless communication and encryption

Resulting in:

- Greatly increased vulnerability (at least initially) to both simple and sophisticated attacks

PREDICTIONS

- Covert seals and nano-seals become important (secret and hidden)
- Tags and seals based on complexity become more widely used

Resulting in:

- Good cost and vulnerability performance, but only to the extent that problems with information secrecy can be controlled

PREDICTIONS

- Container security and tamper-evident packaging receive more emphasis
- Further blurring of the distinction between tags and seals
- More sophisticated seal users
- Terrorism and industrial espionage drives seal use and development
- Cheap, low-tech passive seals continue to be important
- The simplest, most effective tags and seals will be made from high-tech exotic materials (e.g., polymers, composites, biomaterials, nano-crystals) with minimal use of electronics, microprocessors, or electro-optics

I think this is what we will see in about 20 years:

- You get better security using simple seals based on high-tech exotic materials rather then seals based on complex electronics.

Bottom Line: This 7,000+-year-old profession has a lot of life left in it.

STANDARDIZATION/FEDERAL SPECIFICATIONS OVERVIEW

Mike Farrar, DoD Lock Program Technical Office,
Naval Facilities Engineering Service Center
Port Hueneme, CA

In 1993 Secretary of Defense, William Perry, initiated the spec reform program. The primary focus in defense standardization has been the conversion of military specifications to industry consensus standards, commercial item descriptions (CID), or performance specifications.

As of October 1998, the following results had been obtained:

Specifications canceled:	7,715
Standards canceled:	737
Documents inactivated:	6,162
Non-government standards (NGS) adopted:	2,209
Commercial Item Descriptions published:	679

Many Federal Specifications used by DoD were under close scrutiny also and Geneeral Services Administration (GSA) had already undertaken a program to replace all Federal specification prepared by civil agencies with industry standards or CID. That action didn't immediately apply to Federal specifications prepared by DoD activities, and DoD initially focused its attention on the military specification and standards. However, in August 1998, Defense Standardization Program (DSP) policy was issued stating that DoD prepared Federal specifications were to be canceled, inactivated for new design, or replaced with an NGS, CID, or other appropriate document. With adequate justification, some Federal specifications may be kept active. By the end of calendar year 2000, any documents for which one of these actions isn't taken, will be canceled at that time.

The result of this action combined with already progressing spec reform initiatives is that by the end of calendar year 2000, every spec and standard prepared will have been scrutinized with the goal of eliminating any unnecessary prescriptive requirements. The result will be procurement based more on performance and less on design. This should be a good thing, but there are many areas of Government procurement that require close scrutiny of the products purchased to be sure the warfighter isn't holding a non-functioning weapon or tool when the bullets are flying.

The tide of specification reform doesn't seem likely to change, so it means each participant in the logistics process will have to increase his or her vigilance in making sure the products meet the needs of the user. This isn't going to be easy. There has been some fallout from specification reform that probably wasn't intended. First, many service activities have been lead to believe that DSP is dead and they needn't invest their money in it anymore. The result is a large portion of the documents that still exist (there are many) are being transferred to the Defense Logistics Agency (DLA) activities resulting in the buyers writing the specs instead of the users. Of course, the intent is still to coordinate the documents with the users, but within the services, each DSP preparing activity managed that effort for a portion of the coordination process. Loss of this shared responsibility is putting tremendous burden on DLA without a

corresponding increase in resources. In addition, the trend toward working capital funds (formerly DBOF) means a strong likelihood the users won't be able to put adequate effort into spec review when they're coordinated, unless funding is provided for that effort. The upshot is that there is still much work to be done to create some balance in spec reform.

Not only have the documents been changed significantly, but also the organization guiding DSP has been restructured and moved. Once a part of the Office of the Under Secretary of Defense for Acquisition and Logistics, that office now maintains responsibility for overall policy guidance. The Defense Standardization Program Office is now a part of the Defense Logistics Agency (DLA) and reports to the Director, Logistics Management in the Defense Logistics Support Command (LSA).

Within the Naval Facilities Engineering Comand (NAVFAC), as of 1 October 1998, there is no longer a DSP preparing activity. YD1, as it was identified in the DODISS, was disestablished on that date. Following the termination of funding DSP, SLC reached agreement with other standardization management activities to transfer about 80 percent of the specifiactions they had prepared.

- DISC Philadelphia about 40 percent
- DSCC Columbus about 25 percent
- DSCR Richmond about 15 percent

Army Tobyhanna took the five packaging documents as well as all background files for specifications in the PACK area. Philadelphia also assumed the lead standardization activity responsibility for 12 of the 21 federal supply classes.

They have asked Navy DepSO for direction for the following:

- Further spec transfers
- Documentation required other than DD forms 1865
- Permission to cancel those not transferred
- Disposition of background material not transferred
- LSA for the remaining classes

If you need information about current DSP initiatives or activities, or are interested in getting information about a particular specification, the following web sites may be of interest to you:

- Acquisition Streamlining and Standardization Information SysTem (ASSIST) is available to search for, view, and download official, full text PDF versions of Military and Federal Specifications and Standards, Commercial Item Descriptions, Qualified Manufacturer's Lists and Qualified Products Lists included in the DODISS. There is no charge for registration or access to the documents. Registration information and procedures are given on the web site at http://assist.daps.mil.

- Other general DSP information, including the Standardization Newsletter, is contained in the DSP web site at http://www.dsp.dla.mil.

During the presentation the following was discussed between Richard Williams and Mike Farrar.

Mike Farrar: It is my understanding we would need to get approval from the DSP in order to keep a spec, is that correct?

Richard Williams: I'm not sure that is correct. You need a sponsor and interface. Let me make sure I understand this idea, you would have to have a number of Government standards, so depending on what it is would have to be justified, done on a case-by-case situation. The general idea is to go with the commercial standard.

Mike Farrar: Protecting our arms and other special weapons. This needs to be considered. The TID specification reform doesn't participate in the logistics side. We will have to increase vigilance for the product to meet the need of the user. So many times this doesn't happen. You have buyers out there that don't have a clue about locks. Somebody says get me this type of lock and they figure another is similar, but it doesn't meet the requirements.

Richard Williams: What if we gave you that responsibility?

Mike Farrar: We would be more than happy to, for security products.

At the end of the presentation these questions and concerns were conveyed.

Tim Besse (CSSG)**:** If we are going to accept commercial specifications are we going to have a requirement that they be Underwriter Laboratories (UL) tested or some other independent laboratory tested?

Mike Farrar: Why would you want that? I can't see any real benefit in UL testing. Based on my own knowledge. Eric, you have any thoughts of this?

Tim Besse (CSSG)**:** Like with GSA products, GSA will require UL testing or similar testing.

Richard Williams: UL is nothing more than a commercial testing organization. They pay for vendors. Our position, from a policy standpoint, is to recognize the established organization has some standard that you can stand up with and say, that is a correct standard. Anything that is an established standard, at least you hope, you know what your are getting, know that doesn't always work. When you choose UL, you are choosing a commercial test organization from other industry based commercial test organizations. From our standpoint, we would want to know what the commercial test standard is. Specifically, how do they go about their testing procedure, and more importantly how they monitor once they put their model on it. We want to be sure that unit 79 (i.e., down the line) is as good as the first unit. So, there is benefit of having people like UL do it. The reason is you have too many problems is because of instances of where people are trying to check alarm systems that don't have the background. At least if you have a UL stamp you know you have something doing some kind of given level inspection. I would like to see a similar type of thing on other products coming from the Government. The key is you have to

establish what your requirements are to start with. Problem of difficulty on seals is from how do you defend against covert attacks.

Eric Elkins: The Government testing programs, on some of the items we test, is exactly as what Mr. Williams is mentioning. We know or we have a pretty good idea that we have consistency in the products. They don't just test once. They watch the assembly line, and pick one at random for re-testing. They want to keep the quality control up. If not, the assembly line will be shut down. If shut down, they have to go through the whole thing again.

Mark Hayward (Encrypta Electronics)**:** In the United Kingdom (U.K.) there is a British standard on security seals and we manufacture our products to that standard. This is tested in order and they do exactly like Mike is suggesting. They come in, collect a sample, at any time, identify that and go and test it. This makes sure that everything we produce, when we say it meets a British standard, they accredit it and assures that it does. I don't see any reason why you couldn't run the same type of operation here.

Mike Farrar: Exactly.

Richard Williams: Could we get the British standard, if we could just look at it, see if you cover everything that we have. This would be helpful.

ASTM ELECTRONIC SECURITY SEAL STANDARD EFFORT

Bruce Roberts
Chairman
ASTM F12.56 E
Electronic Security Seal Task Group

I am a vendor, the Federal Marketing Manager for Encrypta Security Seals. We invented the electronic security seal about 15 years ago and have been busily trying to interest Government and commercial customers around the world. Because of my location in the Washington, DC area, I find myself involved in numerous professional and security organizations. With your permission I would like to tell you I am the chairman of the National Cargo Security Council (NCSC), Board of Directors. I have brochures available on NCSC if you are a security professional either in the commercial or Government world. I invite you to come play with us, if you have any interest in the world of cargo security, this is the organization to join. I also happen to be the Chairman of NCSC Cargo Security Technology Committee. So for you vendors that have new and exciting products that could be applied to cargo security, my committee is designed to alert the cargo industry about those new products and technologies.

Purpose: 1992 British Standards Institute (BSI) issued a new security standard BS7480. This included language defining and describing electronic security seals. BS7480 was soon adopted by European Union, which many of our NATO members are part of. For the last three seal symposiums we have been bouncing back and forth off standards and specifications. At the last seal symposium Mike Farrar announced that he and his associates were working to develop a DoD guideline on security seals that would include electric security seals. At the time, Mike indicated that he and his associates would welcome an American Society for Testing and Materials (ASTM) initiative to review the BSI work on electronic security seals. To determine whether or not ASTM should adopt the BSI electronics seal language or develop one of its own. Based on that, I made a petition to ASTM to request they form a task group to look into this operation. They agreed and made me the chairman of that task group.

My sad story, October 14, 1997, the F12.56, "Electronic Seal Task Group" was formed. Members included:

- 6 seal manufacturers
- 2 DoD organizations
- 1 security consultant
- 1 electronic lock manufacturer

We invited as many seal manufactures as we could to join the party. I sent out copies of the ASTM Standard and BSI Standard, also to the Australian's and the New Zealander's. I made continuous mailings to committee members, with no response. In June 1998 I made an executive decision, I pulled the plug on this task group. At this point, ASTM has eliminated this task group from their roster. At this time, there is no task group working on electronic security language for ASTM. My recommendation, as the former task group chairman, if the DoD has a need to adopt

an electronic security seal standard that they consider utilizing the electronics seals language contained in BS7480. Since that standard is already approved, the European Union, and all of our NATO allies in Europe have adopted it.

Question: Is the only way to get this standard is to buy it?
Answer: No, if you would like a copy, give me your card and I will get you a copy of it.

Question: During that time period you are talking about I was finishing up a Sandia report on active seals technology. I use to be a member of ASTM and pushed for a fiber optic seals standard. It had the same results as your task group. However, I was never contacted. I contacted the BSI, I have a web site, and they would not allow me to get a copy or overview of each standard so people could go to my site and share in information on the web. Bottom line, they wanted money, so I walked away from it.

Bruce Roberts: One of the advantages of working for a British company is one of my directors also happens to sit on the BSI Seals Committee so we can make that information available to you.

Bob Loughlin: It seems to me that when the Navy's standard didn't get picked up this is a repeat of the same thing. ASTM, being the consensus organization that it is, membership has to take the initiative to make this happen. I think there is a mechanism, should you choose to use it, address the main committee (F12). Make the point that there is a BSI Standard that should be accepted, as is, to put in place to serve the market place as it is being represented by the interest here.

Eric Elkins: From the DoD side, the biggest problem that you are having is that we do not have a requirement to use electronic seals. Since we do not have a requirement and they are more expensive to use than the other seals we have, there is no motivation for DoD to get involved with this or to adopt the standard. Mr. Williams is asking us to look at higher tech seals. I think this may be down the road, this may be something we are a little premature on. There is no requirement on any document that I am familiar with which says we have to use electronic type seals. When there is, then we will need a standard to go by.

Bruce Roberts: However, there are a number of DoD organizations that are currently using electronic seals and I can't tell you how or why they are using them.

Richard Williams: What I propose you to do from here, is try to drive the standards up from the bottom as opposed from coming down from the top. Politicians don't want to spend money and that is basically it. If I were designing this I would suggest

- That the Government is responsible for seals to some extent, get together with industry, and put together an advisory service. We can't give you that authority, you can do that on your own. You put together what you suggest as a standard and applications for the standard, send that up to the Office of Secretary of Defense (OSD). Then we will take a look at it and see what we can do with you. Join together

as your advisory structure. If you want to draw on the English standard, which is what you propose, I think they said that was a public standard.

Mark Hayward: It is a published public standard. But the British make their money by buying standards, if you can believe. So you would have to buy the standard, the cost about $30.

Bruce Roberts: ASTM also charges you for their standards.

Richard Williams: In a partnership then you would be apart of it, which would allow the Government to draw on the industry. After you join together with us on the development of something, which you can use. Come up with some really good ideas, which would be very realistic and correct applications. Now is the time to come up with different ways to suggest this.

Question: What are these specs telling us? What do these standards established?

Bruce Roberts: They (BSI Standards) define what an electronic security seal is, but it doesn't establish a specification. It establishes testing procedures, what those testing procedures should be (i.e., environmental, etc.).

Question: Once something is tampered with is it ever re-tested?
Answer: Yes, this meets the BSI Standard, and we can test anytime.

Randy Cabeen (TRW)**:** When you talk about these tampering standards, how does it take into consideration new technology, new methodology, etc., which can introduce new vulnerabilities. Is the standard continuously updated or do they come in and re-test, re-rate your system?

Answer: With what little I know and with working with ASTM, what I understand about the BSI, every standard has a drop dead date. They automatically review standards on a regular basis every 3 years (UK). They look at the existing standard and compare with new developments.

BY-PASS THE SEAL AND STEAL THE CARGO

John Tichenor
Cigna/Marine Risk Management Services
Jersey City, NJ

My presentation is a "how to presentation" on how to steal cargo from ocean containers (without breaking the seal). In some parts of the USA and the world, it is easier to steal some of the cargo without breaking the seals than it is to steal the whole container. This presentation will take a "how to" approach from the perspective of a Marine Cargo Surveyor. Knowing how "thieves" steal the cargo can lead to better seals, and sometimes to catching the "bad guys."

PRESENTATION:

Who, what, when, where, why, and how much money? These are the questions that I am called upon to answer in the course of my job as a Senior Staff Cargo Surveyor for one of the world's largest marine cargo underwriters. I would like to teach you how to manipulate the seals or by-pass them to enter an ocean container and steal the cargo and not get caught.

Pirates! Swashbucklers! Are still boarding ships and stealing our cargo. Yes that cry is still heard in certain parts of the world; the Straits of Malacca, South China Sea, and off the coast of Brazil. However, most cargo is now moving in 20- and 40-foot containers and today's cargo pirate is not going to have a sword and an eye patch. Now we call them "thieves" and they will be wearing Rayban sunglasses, driving Freightliner trucks, and educating each other with cell phones on how to tamper with, or by-pass the seals that you are using, designing, or manufacturing.

Start with a good understanding of how ocean cargo moves. You will quickly learn:

- Where the seal are applied
- Who applies them
- Where the seal numbers are recorded

The best cargo thieves have the knowledge to defeat your seals, and they have a good understanding of international trade. The golden triangle, Miami, New York, and California.

Ocean containers have four vertical locking bars on the two rear doors and four places to put seals. You have to open the right hand door prior to the left hand door, so on the right hand door handles is where you should place your seals. Approximately 70 percent of the containers have Bloxwich hardware and the seal is applied through the hardware. Approximately 20 percent have Powermatic type seal keepers and the rest? The first seal is typically applied at the shippers loading dock and this can be the thieves' first opportunity.

The following are eight different types of opportunities that thieves can use, with police notes:

One: In route to the shippers warehouse, the thief removes the rivet that secures the door handle to the vertical locking bar and replaces it with a two piece post that screws together and has the appearance of a rivet. The cargo gets loaded and the container gets

sealed. Down the road on the way to the port you stop, unscrew the post, open the doors, help yourself to the cargo, close the box and continue to the port. Don't forget to add some weight to compensate for what you took out. In order to properly load the vessel it's important to know the weights of the containers; so in addition to the weight listed in the shippers documents the containers are often weighed as they arrive at the pier/terminal. Cinder blocks and bags of sand work well. (*Police note: University Geology Departments can help you identify the country of origin of sand and cinderblocks*).

Two: Bring your own blank seal with you and stamp it with the number that the shipper uses on his seal. The person checking the seal at the port will not know what type seal (e.g., bolt, band, wire) was used by the shipper, all he is concerned with is the "number" …does it have the number that is listed on the documents: (*Police note: Bolt type seals make the best blank seals… grind off the number, polish it, get a stamp set in a hardware store, and add your own number*).

Three: Dental floss. Keep a package handy and if the loading dock supervisor is lazy, he won't want to jump down and apply the seal, but instead will hand the seal to the driver and watch him put it on - or maybe not. With bolt type seals, it is possible to wrap the seal with dental floss that fills the notch that causes the seal to engage. You push the seal together, then head down the road and pull it apart (you know the rest), reseal and make delivery at the port. You can take the dental floss and jam it in. This trick can often work when the container is on the other side of the port. Here you have to be on the lookout for a lazy loading dockworker that doesn't want to climb down and cut the seal. He hands the cutters to the trucker, of course the trucker has already cut the seal and stolen some cargo and is now only appearing to cut the seal. (*Police note: Loading dock worker will never admit that he was too lazy to climb down cut the seal and handed the cutters to the trucker*).

Four: Shipper places two seals on the container one on the right hand door and one on the left. Documents show only the seal on the left-hand door. A real gift to the thief. Cut off the right hand seal, steal some cargo and reseal with your own seal, documents will still show seal integrity! Where do I get my own seals? Keep your eyes open! At many locations that you will be visiting as a truck driver you will see the box of seals is left out in plain sight, free for the taking. And when the dockworker says, "Hey Joe, grab a seal from that box on the shelf, What's the number on that?" Make sure you have picked up several, never know when you might need one!

Five: Next opportunity to open the container occurs at the shipping port terminal. "Cargo at rest is cargo at risk." Opportunities here vary with port security conditions around the world. The containers onboard for a long period of time and stowed below decks as a thief you would have plenty of time and privacy to open a box and pilfer cargo. While this is true there are some things working against you. You can't really get good access to box doors when containers are stowed in the cells onboard most container vessels. Even if you could get the doors open and steal the cargo you'd still have to get if

off the ship, past customs agents. Except for box of lobster tails or shrimp which the crew can enjoy en route. This is not a good plan! Keep it moving, stored below deck, after you steal the cargo, get past customs.

Six: Next opportunity to open the container occurs at the receiving port terminal. "Cargo at rest is cargo at risk" and your opportunities will depend on security. At most US ports security at terminals is good. Will the seal be checked here? Yes, sometimes as the container comes off the vessel, and always as the container leaves the terminal it will be checked against the documented seal number. Will the container be weighed? No, not routinely. Get yourself a job as a longshoreman and you'll have easy access. However, this is easier said than done. These jobs are $100,000 plus a year and if you had one you might not want to put it at risk trying to steal cargo, then you have to get the cargo off the pier. Security at port terminals is good. The better way, delivery to the consignee or the receiver. Attention: This is the best opportunity for you to steal the cargo.

Seven: Easiest way. Steal a car, drive the car into the truck that has just left the port with a container and chassis. When a driver gets out point a gun at him and steal his truck. "California Style-Cargo Theft." Too Risky. What if the driver has a bigger gun than you do? This is too risky so I recommend the following:

Eight: "Classic East Coast Style, Leaker Loads" a much safer method and while you don't get as much cargo each time you can most likely repeat your actions many times. You have learned up to this point that there are lots of opportunities, and lots of people and places to point fingers at. If you don't get too greedy they will never suspect you. Because you'll be the truck driver and everybody knows truck drivers wouldn't steal just a little - they would steal a lot.

That's eight good ways to get the cargo without breaking the seals and if anyone knows how those mythical "guys at the piers" can get the doors off the hinges, please let me know.

Question: Are shipping containers monitored on computers?
Answer: The steamship companies monitor them with computers. They are leased by leasing companies so individual line owns so many boxes outright and so many boxes are leased. Remember, just the box, not the chassis.

Question: Are the cargo shipments on a network that can be hacked into is my question?
Answer: The best way to get information is to ask people on the piers, handling freight loaders and pass that information on.

TAG/TID APPLICATIONS FOR ARMS CONTROL –

Major Greg Louden
US Army
Defense Threat Reduction Agency
Kirtland AFB, NM

DTRA Information Briefing to the DoD Security Seals Symposium

Purpose: Provide an overview of the Defense Threat Reduction Agency (DTRA) interest in Tag/TIDs for arms control applications.

TOPICS

- DTRA Arms Control Technology Division
- Joint DoD/DOE Integrated Technology Implementation Plan (Joint I-Plan)
- TID Testing for START III
- Summary

Defense Threat Reduction Agency is the newest DoD Agency, we stood up on October 1, 1998, and Dr. Jay Davis is the Director. Four different distinct DoD Agencies formed us:

- Defense Special Weapons Agency – used to be Defense Nuclear Agency
- On-Site Inspection Agency – this is the element my site falls under
- Defense Technical Security Agency
- Office of the Secretary of Defense Elements

JOINT I-PLAN

- Joint DoD/DOE Integrated Technology Implementation Plan - Provides coordinated and comprehensive framework for a program of technology implementation activities to support U.S. efforts directed toward current arms control and nonproliferation agreements
- START III – main focus
- Mayak Transparency - threat reduction
- Trilateral Initiative – series of agreements between U. S. and the Russians
  - Plutonium Production Reactor Agreement – coordination efforts
  - Plutonium Disposition Activities – coordination efforts

DoD/DOE STEERING COMMITTEE

- Technology Assessment Working Group
  - Radiation
  - Tags/Seals

    - Alternate Technologies
    - Remote Monitoring
- Information Barriers Working Group
- Vulnerability and Security Analysis Working Group

TID TESTING FOR START III

ROLES OF TAGS/TID –

- Monitor total nuclear weapon inventory
- Monitor strategic nuclear weapon inventory at declared locations
- Monitor nuclear weapons at storage sites
- Chain of custody of nuclear weapons components
- Confirm closure of facilities
- Inspection support

SELECTION CRITERIA

- Technical Performance
    - Accuracy
    - Spoofability
    - Maturity
    - Exportability
- Operational Requirements
    - Inspector friendly
    - Reliability and maintainability
    - Operation impact
- Acceptability
    - Safety
    - Intrusiveness
    - Negotiability
    - Cost

POTENTIAL START III TIDS

- Tamper tapes
- Active electrical loop seal
- Fiber optic loop seal –
    - Active
    - Passive
- EID Button – electronic ID buttons
- Polymer/Metal Locking TID

Types of Testing – Randy Cabeen will be conducting these later this summer

- Environmental tests and evaluation
  - MIL-STD-810E
  - Peacekeeper Rail Garrison System Specs
- Operational tests and evaluation – looking at how easy is the technology for a non expert to learn to use and inspect
- Adversarial analysis

CONTACT INFORMATION

Major Greg Louden
DTRA/OSTS
505-846-9615
DSN 246-9615
Louden@ao.dtra.mil

RADIO FREQUENCY IDENTIFICATION

Lynn Torres
Naval Facilities Engineering Service Center
Port Hueneme, CA

A team of engineers at the ESC has been doing a variety of things over the last five years in Radio Frequency Identification (RFID). Though the primary direction from funding agencies has been to focus on the logistics applications in the military mission, some of the knowledge gained is directly applicable to security, or could be secondary benefits to security. Most of the work focused on RFID work at the ESC has been directed toward the military or tactical application of these systems. The most significant lessons learned in these years of development is the necessity to take a systems approach and to separate the RFID system into its logical components of the data source, the communication link, and the information management system.

BACKGROUND WORK

- Air Force MITLA Program – DoD use of RFID started with this program. Micro Circuit Technology and Logistics Applications (MITLA) is run out of Wright-Patterson Air Force Base, Dayton, Ohio. They were looking at a broad spectrum of RF technologies. One of the applications they focused on was business process engineering. As an implementation sight at Kelly Air Force Base (AFB), they employed radio frequency tags to measure and control the rebuilding process of jet engines as they went through their depot facility. This allowed them to match components at the end of the maintenance repair cycle with the original platform, making sure that the right parts were returned to the right craft. This also helped them to really refine whether the business process was efficiently working in the manufacturing sense. The RFID information management system identified choke points which could then be addressed through new methods in process flow management.
- United Parcel Service (UPS) Truck Manegemtn in Lots – In this commercial application test, UPS utilized the Savi RFID technologies also being tested by the military. Each truck had an identifying tag which allowed a truck entering a compound to be identified and registered in a hands-off fashion. The automatic logging of vehicles entering/leaving the compound facilitated not only process flow monitoring but also supported security issues in the facility. The commercial saving of the 3 to 8 minutes of each truck through the gate, saved by eliminating the manual check-in process, showed substantial savings over time.
- Rail Car Security – Hauling military assets over land lines by rail has historically been conducted with manual security features in place. One of the things the military and some commercial outfits do is put all of the ISOs end-to-end on the rail cars. This prohibits anyone from opening the doors during transit, while the rail cars are sitting out in the field, or in uncontrolled lots. By using RFID technology, rail transport customers could put tags on the car doors providing some sort of sealing function.

The containers could then be transported with the door ends exposed, making authorized access for supplies and equipment easier.

- Signature Card Upon Delivery – As interest in using the RFID tags for tampering devices grew, Savi Technology and Texas Instruments, as well as others, worked on developing a key card, allowing someone to officially take receipt and log into the RFID memory that they had accepted a delivery. This RFID memory card would retain a record of who had accessed and possessed an item in its history. Each authorized receipt party may have a small signature chip which uniquely identified them or their duty station.
- Positive Baggage Matching – The ESC has been working with the private sector and the Federal Aviation Administration (FAA). Airports are increasing security to include the checking of luggage. No luggage is supposed to be transported on a flight without the owner of that luggage making the trip at the same time. On international flights this is already in place with RFID technologies, but it is largely facilitated by luggage being put into containers for ID purposes and by the longer check-in lead time requirement. With positive baggage matching, your luggage states you are seating in row 19A and if that person isn't on board, they remove the baggage from the cargo hold and allow the flight to depart on time with a matched person/baggage manifest. The FAA is looking at RFID technology solutions to the security issue of associating a passenger with luggage, and identifying where that luggage is in the cargo hold. Discussions also include bar code stripes and the cost of the ID technology, presenting a challenge to industry.
- Choke Point Management – The most commonly employed military management activity by RFID technology is choke point management. This is done with both active and passive tags. Data content of the tags has also varied greatly in different system tests, ranging from a license plate on a passive tag and serviced by a relational database to an active tag with full manifest data in a more object-oriented type architecture. The Army supported their retrograde out of Germany with this type of technology, and the same tools were used in other European exercises. The military system tests were similar in many respects to the systems currently employed as freeway and toll road choke point controls. The issues with military choke point management systems are that they do not address what has occurred between two points. The integration of this type of system with a tampering system may solve some of the security issues of military convoy movement.
- Marshalling Yards and Ship Offload – The DoD does extensive ship and rail activities, loading items and equipment onto and off of transportation means. The legacy system included placing a colored placard on each item so when it was off-loaded a driver would know what location it was to be taken to, or who was its owner. RFID not only offers opportunity to make this a more sophisticated system but also can increase the ability to rapidly predict readiness of a unit based on how much of its equipment is in place.
- Packaging, Tagging, and Mobile Loads – The DoD wants to be able to associate smaller end items into larger aggregated loads using RFID technology. Smaller items, some of large value, are placed into larger modules and onto transport vehicles. The RFID technology would allow you to make these associations and actively track the

issue of these items. Eventually, this would lead to an ability to anticipate the resupply needs by allowing someone to "count" expenditures or issues of individual end items.

DOD CONSIDERATIONS

- Sensor Information Relay (SIR) – Employing a single capable architecture that can tell you where something is and its status (e.g., temperature, operation, status, location,etc)
- Record jackets – Volumes of data associated with a principle end item showing the life cycle of an item to include its maintenance and its ownership.
- Identification friend or foe – timeliness – a significant design issue when the data you need is now becoming real time necessary vice near-real-time.
- Lot records – Knowing what assets are located where across a marshalling area or a battlefield or within a theater.
- When things get checked in – Tracking units of issue and item availability for use
- When maintenance is due – Notifiers or triggers to signal a status change in an end item
- What you have to do – Giving some signal transmission of the necessary service needed
- Temperature sensing - Medical, in or out of the tolerance, prognostics
- Tampering indicators – Has someone moved it, when it happened, how it happened, SIR
- Warehouse management – Cost is a factor. Desire a system that goes from warehouse to battlefield with a single hardware/software infrastructure
- Parent/child relations and objectified battlefield – Relational databases, rapidly changing relations, and association of items to other activities going on in the battlefield.

DoD UTILITY OF RFID

- Asset visibility
- Warehouses
- Choke points
- Battlefield Situational Awareness
- Sensitive materials control
- Movement Control
- Better Business Practices

RFID IN THE MILITARY

- A systems approach needs to be taken
- Hardware components – Select active or passive components

- Communication link – Using a military communication network without a special infrastructure
- Ties to an information infrastructure – Can't be a stand-alone system. Need continuity for a warehouse or industry visibility to the consumer solution, with this consumer often being deployed.

RFID HARDWARE

- Passive tags – From bar codes to passive response tags
- Active tags – Drives up the cost because of batteries, and brings into issue the battery life cycle management and battlefield security of controlling information transmission.

There is a significant balancing act between the issues of capability and cost. There is yet to be a real component that industry and DoD agree can meet all of these functions. It is perhaps not reasonable to make all those function in a single system. But a systems approach to merge the ranges of capability into a single top-level view is necessary.

COMMUNICATION LINK

- Existing infrastructure is desired, requiring no special systems to be placed on the battlefield due to additional training required and additional hardware costs, as well as battlefield system complexity.
- Bandwidth consumption is a concern in the deployed environment, requiring the system to send only decisions or small bits of data as needed.
- Foreign considerations – (is that bandwidth authorized in foreign countries?) For all training other than a war.
- Information security – RFID lends itself to data being distributed and the communications links of RF are open. The military presently requires hardware encryption vice software encryption. At some point when enough data is aggregated it does become classified as information.

TIES TO THE INFORMATION INFRASTRUCTURE

- Legacy Command and Control
- Automation of Manual Processes
- Elimination of Stove Pipe Mentality

OTHER CONSIDERATIONS

- Systems Approach – They want something that will work in:
  - Warehouse to Garrison to Battlefield
  - Security and Records and Captured Sensor Feeds and Command and Control
  - Total ownership cost – Buying the hardware and its lifecycle costs (batteries?)

- Non-proprietary software developers kit – Tie to the information infrastructure
- Data centric functions – What is out there?

Question: Even if the enemy does not have the ability to gain the RFID information (due to encryption), can they still use the "transmission" to get a location and make it a target?
Answer: The military has talked about tags as discrete sensors across the battlefield. The tags presently produce a very low kilowatt reading. You would have to be in close range to the RFID tag source to identify its location. The RFID sensor data rapidly links to a higher communication infrastructure that probably has significant protection. With this architecture effect, each tier has a higher security level in place.

RFID has primarily been considered by the military as a logistic application. The old deployment style, where logistics is typically in a rear secure area, RFID signature is not a significant consideration. But as logistics got to the distributed battlefields, logistics data is critical and the information security issues become more valid.

RFID information security is a growing issue. Discussion of how far the signal travels, under what conditions, can you control the radiation radius, and can you trace the source location continue to arise. At the same time the DoD sees a possible need to boost the power on RFID tags to do truck-to-satellite communication, giving an increased military capability and getting out of the choke point management scheme, but at the cost of more power signatures and causing a larger security issue.

As concepts of employment mature and technology becomes more available, a real determination of what system capability is needed will emerge. Likewise as logistics functions, largely employing the RFID technologies, become a more active part of the unsecured battlefield their need to comply with information security standards will become more structured.

SECURITY SEALS, RFID TECHNOLOGIES AND THEIR APPLICATIONS

Kim Rasmussen
OneSeal Inc.
Whippany, New Jersey

A small important detail in shipping – A padlock intended to be opened by a bolt-cutter.

In the early days of container shipping, all containers were closed and secured by ordinary padlocks with keys. But the key for a padlock on a container presented a problem as the keys were often delayed or lost at final destination. This caused Michael Remark to invent a locking device that had to be cheaper than a padlock but with the same security.

Michael Remark founded his first design in 1974 - the OneSeal A/S. The OneSeal has rapidly grown to become the world's leading manufacture of what is today known as the High Security Seal.

OneSeal A/S is the leader of a world-wide industry and holds its own representative offices in Singapore and the USA, official agents on 6 continents and in more than 30 countries.

When we speak about seals, or more specifically, the manufacturers, our foremost job is not to prevent theft. Theft will occur no matter what we do. Our job is to make theft as obvious as possible to the users of the seals so they can trace back to where things happened, why they happened, and who did them.

ISMA – International Seal Manufacturers Association

SEAL HISTORY –

First Generation

- Proven technology
- Sophisticated technical features
- High-Tech laser engraving, cold or heat stamped, ink-jet printing, or labels
- Many different designs

The first generation of High Security Seals has been improved over the years and today's top model features engraving the seal by use of high technology laser. The engraving is protected by an ultra-sound welded plastic cap to protect against tampering and the seal is finally packed in individual blister packing for easy distribution. All high security bolt seals are engraved by laser beam technology, which prevents tampering and enables production of a company logo on the seals.

Second Generation

- Remote reading/registration of seal number
- Proven technology
- Bar-coding

- Inkjet, label or high quality laser marking
- 100 percent error-free registration
- Software controlled equipment/inventory tracking
- Most first generation seals available as second generation

The second generation of seals - OneSeal commenced in 1991 and introduced the first high security seals ever to be barcoded. The barcoding of seals accelerated sort production and facilitates seal registration by use of hand held computers. The OneSeal Automated System (OAS) features a fully integrated package for using barcoded seals, including hand held computers, staff education, and individual software programs. The perfect solution for container terminals or shipping lines wanting maximum security and where human resources are used for registration of seal and container numbers.

Third Generation

- New technology
- 100 percent error-free registration
- 100 percent hands-free reading
- Increased remote reading distance
- Readable in motion
- Lockable and open user programmable area

The third generation with the OneSeal Transponder System (OTS) - OneSeal has again proven to be the leader within the development of higher security for container shipping. The latest generation of high security seals features the incorporation of an electronic transponder, which allows for fast electronics registration. The OTS system provides users with faster port operation, reduced handling time at terminal gates, and can even provide you with your own container tracking system. Increased security is obtained as the system warns pilferage by alarm. The OTS system is designed for individual requirements, including reading equipment installation and user education.

MECHANICAL VERSUS RFID SEALS

PROs	CONs
Proven technology	Physical contact required
Require physical contact	Visibility required
Tampering easily detectable	No remote reading
No electronic “bugs”	No error-free registration
Lower price	No equipment inventory tracking
	No tampering experience

PASSIVE VERSUS ACTIVE TECH

PROs	CONs
No power source	Less reading distance
No battery	Less user programmable bits
Unlimited life time	No satellite/Global Positioning System (GPS) tracking
Environmentally safe	
Smaller design	
Lower price	

TECHNOLOGIES AND APPLICATIONS

PASSIVE	ACTIVE
Gate or yard check	Satellite tracking
Loading/discharge check	Large programmable user area
In/out registration	Readability exceeding 3 meters/9.9 feet
Reading distance up to 3 meters/9.9 feet	
Ocean/Rail or truck	Ocean/Rail or truck

TECHNICAL SPECIFICATIONS

International standards:	315 MHz
(ISO recommendation)	433.4 MHz
	2.45 Ghz
Passive tag memory:	40 lockable and 35 non-lockable data bits (user programmable)
Passive tag reading distance:	Minimum 3 meter (9.9 feet and readable in motion)
Data communication port:	Standard RS-232 port

INDUSTRY STANDARD

- World-wide ISO standard pending
- Several frequencies required
- ISO recommend three frequencies
- Interaction with manufacturers required

At the moment, no satellite linked seal, multiply design available.

RFID STATUS

- Multiple designs and technologies available/in testing phase
- World-wide industry standard is pending
- The general transport industry is not ready for the RFID technology
- RFID is cost prohibitive for general use

ISMA International Seal Manufacturers Association

- Members include major seals manufacturers world-wide
- Local interaction with authorities
- Interaction between manufacturers on major issues
- Can be used as buffer by authorities
- Should be consulted in major seal issues such as industry standards

Mark Hayward: I was interested that you note that you don't think there is any commercial application for RFID seals technology and yet the previous speaker mentioned UPS was running a system.

Kim Rasmussen: I meant, that generally there are, of course, commercial businesses out there that are using RFID or electronic tags. But if you look at it on a general level or world-wide, the use is really minimal at the moment. That is increasing and will continue to increase at the same speed that technology is developed and the price comes down, before you really see it implemented in depots, containing yards, within shipping lines it is also pending some type of international standard.

CHOOSING A SEAL

Panel Discussion/Presentation
Moderator: Dr. Roger G. Johnston
Panelist: John Tichenor
Panelist: James C. Crabtree
Panelist: James Najar

There is always something that the team is asked a lot about. I think it is real important to be clear on "Definitions." This is the way we have defined the words we use.

DEFINITIONS:

- **Lock:** A device that delays, complicates, and discourages unauthorized entry or removal of items. All locks can be broken.
- **(Security) Seal = Tamper-Indicating Device (TID):** A device or material that is designed to detect, record, and perhaps discourage unauthorized access or entry. (It does not need to resist entry).
- **Tag:** A label, "fingerprint," or unique identifier of an object (or container) that can be used to recognize the object (or container) at a later date, and to avoid confusing it with something similar. (May be applied or intrinsic).
- **Intrusion Alarm:** An active seal that immediately reports tampering (in real-time).
- **Seal Protocols:** The official and unofficial procedures used for seal procurement, storage, checkout, record keeping, installation, inspection, removal, disposal, reporting, interpreting findings, and training.

ISSUES IN CHOOSING SEALS

- Goals – First and foremost, "think this through carefully."
- Likely adversaries – Who are they, what is their motivation, what is the level of expertise?
- Number of seals and frequency of use – Ask questions
- Acceptable false accept and reject rates
- Associated physical security – Dogs and landmines. What seals make the most sense?
- Personnel – Are they motivated, are they highly trained?
- Training – Is it afforable?
- Psychology
- Economics – Unit cost is important
- Time constraints – How long can you spend with a seal for installation and inspection?
- Safety
- Types of containers
- Type of door, hasp, and hinges

- Roughness of handling – How will the container be handled?
- Physical environment – Indoors/outdoors, rain, salt water atmosphere, temperatures
- Duration of sealing - Timeframe
- Speed of results? – Can you afford the time and hassle?
- Post mortem exams?
- Interim inspections without removal?
- Quantitative inspections?
- Covert use?
- Locking and/or tagging functions, too?

It is mostly about fooling people and not the hardware.

I have given you some real simple definitions but in the real world it gets confusing because a lot of security devices have multiple functions. For example, barrier seals, these seals are both meant to be a seal and a lock. In fact almost any kind of lock can work as a seal if I stick on a cheap padlock. I come back and check it and its been smashed or drilled open, that is a type of tampering detection even though the fundamental function serves as a lock. It also gets confusing because seals are used as tags and visa-a-versa. That's because a secure seal has to have some type of unique identification or fingerprint such as a serial number otherwise an adversary could cut it off and replace it with an identical seal. On the other hand, an effective security tag has to have some type of tampering detection capabilities otherwise an adversary could pick up from one object and place it on another.

TYPES OF SEALS

- Active - uses electrical power of some sort
- Passive

TYPES OF PASSIVE SEALS

- Wire loop seals
- Metal cable seals
- Plastic strap (ribbon) seals
- Metal ribbon (railcar-box) seals
- Bolt seals
- "Padlock" seals
- adhesive tapes and labels (pressure sensitive)
- Secure containers
- Tamper-evident packaging
- Passive fiber optic seals
- Security clamps – Cause damage to surrounding material

PHILOSOPHY

- There is no "best" seal.
- There are no "good" or "bad" seals.

There are only seals that fit your goals and resources and require protocols you can live with, and seals that don't fit your goals and resources and/or require protocols you don't want.

KEY FACTS IN CHOOSING A SEAL

- A seal is only as good as the protocols and training used with it.
- ALL seals can be defeated, often surprising easily.
- The unit cost of a seal is not a very good indicator of the security it can provide.
- The unit cost of a seal is only one of many economic factors.
- Tags and seals can be useful even when there isn't a nefarious adversary.

Panelist: John Tichenor
Cigna/Marine Risk Management Services

Well I am just going to touch on a few things. This pertains to ocean containers, freight. When I go in and recommend a seal, the first question I get asked is how much does it cost. People selling seals, give a better rate on the insurance if they use a really good seal. Ocean cargo insurance is pretty good, after a year your rate could go down. In corporate America, like Government, one purchases insurance the other purchases the seals.

- Trade rates, locks, when going through customs – The locks will be a problem.
- Stop entry – Yes both seals slow down entry. Plastic seals can be broken with a pen. A bolt seal is tougher to break open. All thieves know if you get caught with the bolt cutter you get slapped twice (punishment).
- We try to get our insureds to use a bound book for documentation. A bound book makes it tougher to replace a page.
- We try to get them to cut the seal and save, record tracking, throw it in a box, save for two months. Problem is pharmaceuticals use plastic seals, they are not strong enough. The pharmacy manufacturers don't want to take because it is broke, but that is the law. Sometimes the shipment doesn't have the integrity.
- Trade routes, cable seals between vertical ports, in theory we don't know what is inside.

In the corporate world it comes down to MONEY. As the cost comes down industry will accept the new technology. Call up the people and see what products are good, different manufacturers make different products. Call them and I think they will be helpful.

SEALS SELECTION FOR NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY

Panelist: Jim Crabtree
Department of Energy

I work in the area of Nuclear Materials Control and Accountability. Most of our material is in storage, from our perspective, the seal is only one element. We have a number of elements, the two-person rule, personnel security, we have exit inspections, etc., seals are not the only element that DOE relies on.

SELECTION FACTORS

- Environmental conditions
- Type of container – 55-gallon drums, fruit cans, etc.
- Unique identifier – Usually required
- Location of use - Where it will be placed
- Defeatability and detection capability
- Length of use
- Cost – It is a driver
- Ease of use – A lot of environments, we have radiation environments, if it takes the worker a longer time to apply than that is also a cost to us

ENVIRONMENTAL CONDITIONS

- Heat humidity
- Chemically corrosive environments – More of a factor because different containers require different seals
- Radiation background

TYPES OF LOCATIONS

- Vaults
- Glove boxes
- Processing and packaging areas
- In-transit - The most protection, not a factor

LENGTH OF STORAGE

- Days or weeks to 20 or 30 years
- Some seals deteriorate over time – Active seals work on batteries and this is a factor

TESTING BEFORE SELECTION

- Environmental – Chemical, radiation, with drums and containers, move with forklifts you would want a seal that will hold up
- Vulnerabilities
- DOE National Laboratories
- Larger sites do their own testing as well – Oak Ridge, Chris Pickett has done some testing. This is to look at that is specific site.

You want to test it to your setting

SUMMARY SELECT SEAL TAILORED TO NEED

- Use - How
- Environment - Where
- Detection capability – How easy to defeat
- Ease of use – For us this is a big factor but not the only factor

Bottom line: YOU NEED TO SELECT A SEAL TAILORED TO YOUR NEED

CHOOSING A SECURITY SEAL
A PASSIVE ALTENATIVE TO LEAD

Panelist James Najar
ELC Security Products, Inc.

It will be good for the environment to protect your assets, easily defeat and mostly easily counterfeited (passive seals).

BARRIER VERSUS PASSIVE SECURITY SEALS

For most of the last century, traditional methods were the predominant factors in seal acquisition, know the technological evolution of the products. The TID of choice was a lead and wire seal. This low level, tamper-indicating device was applied with a crimping tool, leaving markings for identification. Advanced versions had a second part with an identification number stamped into tin and attached to the wire. Lead seals have become outdated due to studies declaring the toxic properties of lead to be environmentally damaging.

Passive Security Seals were developed as a deterrent to theft and violations of entry. A security seal discourages unauthorized attempts to access the sealed compartments, as it must be destroyed to gain entry. In the event a violation occurs, the security seal becomes the material evidence.

Modern security dictates a re-evaluation of the use of the lead and wire seal throughout tamper-indicating applications. The ease to covertly and surreptitiously defeat, counterfeit, and

otherwise access without leaving traces of evidence has determined that an alternative to this sealing device be found and universally applied.

The differentiation of barrier versus passive seals has been debated for years. Some applications require the need for more expensive physical obstacle means to keep people out, as opposed to the less expensive deterrence of indicating when a violation has occurred. This presentation focused on the need to help determine the best passive alternatives to the lead and wire seal.

Seals – They have to be easy to use, but complex to make, so that they are difficult to forge. Take advantage of the technology available to us.

Be able to retain the unique fingerprint of the seal, resist normal environments. The important part of a seal is the:

- Numbering system
- The identifier
- Hot stamping
- Cold stamping
- Secondary process.

A one-piece seal will make it unique.

Seal Protocols - Part of security system securing our assets, the seal is only going to be as good as the system it is protecting. We make a product that is traceable.

Our company, we feel, has come up with a good one. We call it the "Anchor Seal" it encompasses what I was just talking about. The Anchor Seal is the result of an extremely complex manufacturing process, with high-precision molds operating at minimum tolerance. In practice, the Anchor Seal is easy to use and does not necessitate tools to be applied.

Three basic characteristics give the Anchor Seals their high level of security:

1. The materials used in manufacturing; polypropylene or polycarbonate
2. The closing system
3. The process of individual identification

Question: As technology is moving forward, at department stores they have tracking devices, the technology is there just a comment so that the vendor, DOE, could have the ability to track where this product is going. Something like this could be looked at in the future. Has your company done this?

Answer: We preprint the barcode, mold it into the seal. It becomes a part of the seal in the manufacturing process. It can be defeated like any other. You will need a scanner. The system you talk to in retail, is part of the system.

Question: Just talking about tracking, within a facility. Like in the processing room to a vault. Requires transponder, this is the new technology we will be using in the next century. As Kim mentioned, the costs are prohibited. Money is a driving factor.

Mike Farrar: One of the things DoD is becoming concerned with is how to secure the 3.5-inch floppy disk. A ton of information can be downloaded, put in a pocket, and walk out.

Jim Najar: Securing the disk itself is a software application. You could put a metal detector on it or invisible marking. There are a few Government people using a fingerprint, clear liquid for registration, and use fluorescent paint across the top.

Mike Farrar: In a pocket, OK a single piece of magnetic tape, insert it in the corner.

Jeff Miller: You would have to make sure that the person that was stealing information would be using that disk.

Roger Johnston: We have had a hard enough time with Special Nuclear Signals, you are talking about something more difficult.

John Tichenor: Remember the psychology factor, the biggest deterrent. Could the guard stop me? People fear – They would wonder if it were worth risking their high paying job?

Jim Crabtree: Let me suggest one other thing. I know that if it is a DOE funded project it might be better to check with the computer security people. Develop a directive that the Secretary of Energy will, make it physically impossible to transfer classified material from a classified machine to unclassified one. Come up with a way that it would make it impossible to transfer data between machines.

Jim Najar: Increase the psychological deterrent. If you catch them, you put them away. A lot is when people regret, in fact random searches on people will also help deter other people from stealing.

Comment: Why not just disable the floppy drive if you don't want to have information copied.

Question: Are you aware of the concerted efforts in technology counterfeit? On seal technology that has been counterfeited, credit card copying, in organizations is the same thing going around?
Answer: Yes, on passive seals.

Jim Najar: The technology to create seals is not prohibitive in itself, it is cost prohibitive but you can make your own. We closed down an organization in Africa using the technology we use to develop that seal.

Kim Rasmussen: One of the things you have seen over the past 3 years, most of the high security seals are marked with laser technology rather that hot or cold stamping. Laser is not available in many parts of the world.

JUNE 16, 1999

Eric Elkins - Welcome to the second day of our symposium, the sun will be out soon, and we have a small change to schedule. Everett V. Johnson from OSD who works directly for Richard Williams will talk to us for a few minutes.

Everett Johnson: I just want to say a few remarks about the Lock Program, what we are doing and the relationship to the Seal Symposium. We feel it is important to update you on the Seals Symposium significant accomplishments

- Seals User's Guide, published in 1997, this helps users select the proper seal, apply, control, remove, accomplishment, we have a training program on a video tape. One of the things I have noticed is the absence of the Defense Transportation Command. I would like to know why they weren't here. They do a lot of seals.

What we are doing here: The potential at OSD - We see a variety of manuals:

- nuclear manuals
- chemical
- physical

But they all lack policy guidance on seals. We don't require a specific type of seal. When we mention using a seal it is usually in general terms, no standardization. So if you can help with the policy making, surface a policy that you would like to see in our directives, this is what we would need, from the ground up. Therefore, we can put policy initiatives and policy directives in our documents. I would encourage you to pass any ideas to Eric Elkins so that it will be passed up to us. I appreciate your time.

AUTOMATIC IDENTIFICATION TECHNOLOGY (AIT) AND RFID OVERVIEW –

Susian E. Vickers
US Army Product Manager
Automatic Identification Technology
Fort Belvoir, VA

I am extremely happy to have been invited to your symposium, this is my first visit. I am here for a couple of reasons. I am the Program Manager for the AIT. I am stationed out at Fort Belvoir, Virginia, and we do the RFID program which is the one out in the lobby looking at the equipment. We also have an AIT contract which provides barcode scanning, labels and devices, and printers which could also be of use to the security arena. I have a film that will give an overview of what AIT is and what it does. I would like to bring my focus in on what it is that you do. I understand that security is very important but I am unfamiliar with your arena. To that end when I do contracts I would like to have your involvement so that I can get the types of devices and items on my contracts that will help you meet your mission requirements.

Logistics is key – The Power of AIT. As we embark upon the 21st century, the leadership of military commands, and other federal organizations, as well as private industries, is demanding time savings in the handling of logistical assets. Why the sudden interest? It is not sudden. Managers have always known that time equals money, and when it comes down to the military, time just may make the difference in saving a life, or successful mission accomplishment. This is where AIT proves to be a force multiplier. Though not a system, AIT provides those vital peripheral devices and components that compliment and enables your AIT to save management time and money across the business spectrum. AIT introduces automatic data collection and processes, which supplants error prone manual data entry methods. Using AIT logistical processes from receiving to shipping, to manifesting, and tracking, are now taking hours and minutes instead of weeks and days to accomplish; and routing and rerouting of assets while in transit is made available. That is the true power of Focused Logistics. Real-time not down-time is the new watch words for successful management of logistics tracking and accountability. The power of AIT truly has something for everyone.

Material has to be moved fast, technology is right, personnel want to make things better. Force projection logistics – this is what it is called. Containers sometimes had to be opened, tracking was lost, now we have in-transit and mobility. RF tag is attached to each container.

THE POWER OF FOCUSED LOGISTICS

- Pin-point accuracy
- Total asset visibility
- Flexible solutions
- Business process efficiencies
- Source data collection
- Reduced administrative costs
- Reduced inventory management costs
- Joint Vision 2010 compliance

PURPOSE – Why are we here?

- To introduce you to PM AIT
  - Major functions
  - Value added benefits
- To highlight contract provisions
- To provide insights into the challenges as well as capabilities of AIT in the future
- Provide focus on The Power of AIT for your future which will be made available through PM AIT contracts

MAJOR FUNCTIONS AND SERVICES

- Contracts
  - AIT Contract 1994-1999, Intermec Corp – The AIT contract ends in September 1999 for ordering products. It will continue its maintenance services until March 2004. An AIT II contract will take its place, and is currently in the selection process. With compatibility of existing technologies in mind, PM AIT is ensuring that the same customer oriented products and services will be provided. Like its predecessor, this contract will also offer total logistics management solutions, a 5 year ordering period, and unparalleled warranty and maintenance provisions. The target award period is third quarter FY99.
- RFID Contract 1997-2000, SAVI Technology
- AIT II, fourth quarter 1999 - ? – scheduled to be awarded later this year
- RFID II, ? – No award date as yet, it will be prior to the expiration. We have started working on this through market research, finding competitive and more advance technology to put on.

This is one of the reasons I am here this week. We have the opportunity through the data call, and many of you have picked those up, to expand the requirements that have been put on the RFID contract thus far. I urge you to take advantage of economies of scale offered in a large contract to advance your ideas and your needs to me so that we can put those items on and make them available to you. The current RFID contract offers full warranty for 36 months, with maintenance period following the end of the hardware ordering period. This provides you with the capability of getting devices at a cheaper rate, standardizing within our industry, within DoD, and other federal agencies.

- Program Management – Our office provides program management. We are funded for STAMIS which is a Standard Army Management Information System and we provide full services as a PM. In other words, when I get my commercial item contracts the hardware we take to testing. We evaluate for technical and environmental concerns. We use the performance specifications as required under the acquisition reform revisions. We follow commercial standards. We take a lot of care and time to match commercial standards in the industry with the military standards that we have and thereby do a cross match. When a military use is required and we

can't specify a mil standard, we simply add in that portion of that requirement too our specifications. There is a lot of work done and a lot of expense involved in buying all of the commercial standards, having them available, and making them available commercially.

- Configuration management – Something brand new in the AIT office. We are going into the web for Configuration Control Boards (CCB). This will be accomplished by the web site. The purpose or importance of CCB to you is that we base line our product lines. Then when Engineering Change Proposals (ECP) for hardware and software are required we are able then to get concurrence to insure that the items work and that they are backwards compatible if necessary.
- Site surveys and installation of RF equipment – commercially with contractor support
- ECPs – Also serves for new customers. When new technology updates occur and they aren't on the original contract then the new item can be introduced, this is the method used.
- Test and evaluation – put in place the testing facilities in Tobyhanna to facility the hardware test. Currently testing the RFID equipment.
- Host Nation Approval (HNA) - for approval of frequencies

MAJOR FUNCTIONS AND VALUE ADDED BENEFITS

- Y2K Compliance and Certification – As of December 1998
- Central Ordering Processing Office (COPOs) – PM AIT maintains constant oversight over the other services through the COPOs. Biannual meetings are held to discuss the issues and to conduct training
- Warranty and Maintenance - 2 year warranty, some cases go up to 5 years

INSIGHTS INTO THE FUTURE

- ERP: AIT is looking at private industry for
  - Cost effective knowledge based systems
  - Employ enterprise resource planning (ERP)
  - Integrated warehouse management that includes
    - Inventory controls
    - Automatic picks
    - Labeling versus single stations
- Touch Button Memory: Expanding the capabilities for maintenance, access control, time and attendance, asset tracking, healthcare, temperature and time logging and E-Commerce found in Touch Button Technology.
- Customer service will involve the internet
- AIT is already using our Web page to provide the current AIT and RFID Ordering Guides
- Future contracts will provide greater customer service by using electronic means of performing jobs that require paper today.

ENABLING THE WAY

- Focused Logistics – the Power of AIT. The capabilities of enabling technology found in AIT will be there to meet the needs of the future.
- Requirements of Joint Vision 2010 and the Army's Enterprise Strategy will be met using AIT.

Question: How long or how soon do you need the input for the next contract cycle?
Answer: I am collecting data calls right now, in 3 months this window will close. The data call is on my web site. This is managed and controlled so the data can't be changed and we will have another validation requirement on top of that. The data call that you will see shows the SAVI devices on the current contract. I urge you to take advantage of the last page and add in those seals. Those items that you see can move you to the electronics of security.

PRACTICAL METHODS FOR ENHANCING SEAL SECURITY

Dr. Roger G. Johnston and Anthony R. E. Garcia
Los Alamos National Laboratory
Los Alamos, NM

Enhance Seal Security - A lot of the ideas are little more than common sense, but the traditional problem with common sense is that it is not all that common. I think there are plenty of security programs systems that use our suggestions automatically but I don't think we have seen a tamper-detection program (from out view) that wouldn't benefit from one or at the very least to reemphasizing points that are raised.

Start from square 1 – You can't optimize security if you haven't fully analyzed your situation!

EXAMINE THESE QUESTIONS

- What are you trying to protect and why?
- What are your acceptable false reject and false accept rates?
- What are the consequences of a security failure?
- What functions should the seals serve?
- What are your resources?
  - Time
  - Money
  - Personnel
  - Physical security
- Who are your adversaries?
- What are their resources, experience, and motivation?
- How is your situation likely to change over time and how will you adjust? - Review your goals periodically.

GENERIC VERSUS SPECIFIC SUGGESTION

- The best suggestions for improving tamper-detection are application, program, and seal-specific.
- But there are continuing themes across a wide variety of security programs and seal types.
- Barrier seals need to be used with care - The combined lock and seal functions can confuse matters.
- Seal inspectors should be familiar with the most likely attach scenarios for the seals they are using and look for evidence of them. Security managers don't want to convey this to low level security personnel.
- Encourage seal installers and inspectors to provide feedback, ask questions, and raise concerns. This is very important for communications of security with people.
- Avoid a "shoot the messenger" atmosphere – Inspectors are hesitant.
- Treat security personnel well. Security programs can fail because of disgruntled employees.

- Emotionally and intellectually engage seal installers/inspectors in the task of "catching the bad guys."
- Make it interesting; test and reward seal installers/inspectors; hold contests – Make it worth their while to pay attention.

VULNERABILITY ASSESSMENT OF TAGS AND SEALS

- Discovering and demonstrating ways to defeat the tag and seal
- Suggesting counter measures and ways to make the tag seal

COMPLICATED BECAUSE

- Whereas defeating a lock, safe, or vault involves beating hardware
- Defeating a tag or seal involves fooling human beings.

In 1997 I published a short paper in the ASTM journal of testing and evaluation. (He has copies). What I tried to do in this paper was to summarize existing standards for testing seals for vulnerability.

SUGGESTIONS - VULNERABILITY ASSESSMENTS (VA)

- Conduct periodic vulnerability assessments of your seal program.
- These should be performed by outside, independent personnel.
- Findings of zero vulnerabilities are NEVER acceptable.
- Seals must be inspected just prior to being applied.
- Consider archiving used seals.
- Used seals and seal parts must be archived or thoroughly destroyed. Punching a hole in them is not adequate.
- During inspections, seals should be compared side-by-side with a similar unused seal.
- For the best "before" and "after" comparison for tags and seals, use a blink comparator (superimposed two snap shots). This is a powerful technology because the way the human brain works, in flipping the two snap shots, it will appear as movement. Very powerful technique for finding slight differences between images. The blink comparator can be implemented on computers for about $2,000 of hardware. Using a digital camera and a computer, or for $20 in parts, you can make a mechanical blink comparator.
- The container needs at least as much attention as the seal!
- Carefully protect or encrypt seal data. Don't:
  - Write the seal number on the railcar
  - Store the seal paperwork inside the container being protected by the seal
  - Give the truck driver the only copy of the seal paperwork
- Test covertly for yourself if your seal manufacturer or supplier is protecting your logos and serial numbers from unauthorized purchasers.

SUGGESTIONS FOR MANUFACTURERS

- The (same) serial number should appear on each separate part of the seal.
- Serial number needs to be done deeply.
- Don't sell seals without some kind of logo or serial number.
- Free samples need to differ in significant ways from purchased seals.
- Carefully protect seal logos and serial numbers. Be sure the authorized purchaser is aware of duplicate orders!

FACTS OF LIFE

- There is no such thing a "tamper-proof seal!"
- There is no meaningful seal certification standard. I would be concerned if there were a "seal certification standard" that it would be misused.
- Effective seal use requires a lot of hard work – In the real world.

Question: Have you considered coupling with other technology such as video surveillance with how they handle security of seals?
Answer: Yes, we like that approach. It's a new idea. Traditionally, seals were meant to be in a couple of layers of physical security but traditionally that would be a fence. Maybe there was video surveillance at the portals. But the idea of putting video surveillance on a seal, we haven't seen it implemented much. It certainly is an adversary that makes us nervous. The traditional problem with video monitoring is having someone willing to pay attention to the video. There are a lot of technologies involving motion sensors for video images or other stand alone, and those are interesting. There is a basic rule in security, two or three levels is good, seven levels isn't - gets sloppy attitude. I think an alarm bell should go off questioning that if we have to add the second level of security, what could we have included or done better in the first level? I wouldn't necessarily discourage it, but I wouldn't encourage that having one more level of security is good, because it often makes things worse.

Eric Elkins: Have you looked at the situation that John Tishner talked about yesterday. In an environment where we have the container or a magazine door, are we going to keep it during the duration of the seal. Everything works fine, but as soon as we start having multiple users, travelling through several hands before it arrives to its final destination, and having the container disappear from us then it's a problem because of the different types of seals. Have you considered this in your training or taken a look at how we might improve the process that we talked about yesterday?

Answer: I think that what John was saying was a partial solution to that approach. He was talking about the horrors of who removes the seal, I think multiple layers at multiple delivery spots, be real clear at each location, who is responsible for exactly what, have accountability. At stop number 1 (Bob) is responsible for that seal and has a back up, that is it, nobody else goes to that task. Then someone else will cut off that seal, with complete documentation. What can help is having specific accountability. Pay attention to the seal data, when it goes through different

hands you will have some real vulnerability. Sometimes people add a different seal at each stop. The programs won't overlap.

Eric Elkins: Any recommendation on changes, we manufacturer containers, should we be looking at the design of the container?

Answer: You have to take this on a case-by-case basis and at some point you have to reject the containers. You have to encourage people to reject 5 percent, containers are so variable and containers do change over time. We encourage common sense. If there is a hole in the container, don't seal it, fix it or use a different container.

Eric Elkins: For our security containers we do have them inspected, to see if there are vulnerabilities. It is all apart of the system, a systems approach. Maybe we should start looking at containers that have been tested to a certain standard, to eliminate potential problems. Only use the type of container that, if you inspect it, you would have a better idea if it has been tampered with.

Answer: There really are some wonderful technologies and approaches to doing tampering detection out there. Rivets are a nightmare, there is no excuse to use rusted out rivets. You have to work with the containers you have.

Bart Hanchett: ISO standards for containers, can't those be applied?

Answer: I think they are a little helpful, but a lot of the ISO standards are more about the way a container is constructed and if it is safe for cargo transport. They don't address the issues of vulnerability or questions on how easy it is to pop out a rivet. It's a good start, but it's clearly not quite there.

Mark Hayward: Just to follow-up on this issue, we have sold some electronic seals to a Government department who have actually put them on the inside of containers and hooked them up to sensors, so they may have a bolt seal on the outside but an electronic seal on the inside so that if somebody cuts into it and welds it back up, this will record the tampering, linking it to a light sensor or movement sensor. I am just suggesting, like Eric mentioned, you could hook up two different technologies. The mechanical seal on the outside to deter anybody from getting in and the electronic on the inside which will record if anybody has tampered with the cargo.

Answer: That is a good approach. The problem is with the seals, if the adversary goes through the container, your happy, but you haven't fixed the security problem.

TALKING SEALS

Mark Hayward
Encrypta Electronic Security Seals,
Wales, United Kingdom

How Much Is Sealing and Stealing Costing Your Company - I want to provide information to you with our current technology, with the way we are going, and with developments in the U.S. and also with the U.K. Last year the National Security Counsel was here and talked about the annual U.S. cargo theft of $10 billion of loss in the U.S., this is only an estimate because very few record this information.

NEW TECHNOLOGY INTELLIGENT ELECTRONIC SEALS - WHY

Electronic Security Seal With Read/Write Tags

- Improves load security
- Simple automatic trailer status verification
- Eliminates disposable seals
- Built in audit trail of activity
- Reduces manpower
- Integrated with vehicle management systems

APPLICATIONS

Contract distribution, bulk food tankers, petrochemical, multi drop deliveries, and trucking. (Load temperature monitoring available soon).

WHAT IS AN ELECTRONIC SECURITY SEAL

- Rugged battery powered device
- Unpredictable random seal number
- Simple and maintenance free. If you can press a button you can work this electronic seal
- Life 4 to 6 years – Some can go up to 10 years
- Time and date - 50 event memory
- Downloadable data

SECURITY BENEFITS

- Unpredictable random numbers
- Numbers not generated until seal is closed – Major benefit
- Permanently fitted to equipment – Advantage because there will be no excuse not to seal it

COST BENEFITS

- Eliminates disposable seals
- Reduce administration cost

INFORMATION BENEFITS

- Built in audit trail of activity proof of delivery (POD)

CRYPT DATA - Event seal close open length of time, management information

- Real-time and date logging
- Downloadable information
- Management reporting software
  - Asset tracking
  - Security violations, etc.

HIDDEN BENEFITS

- Safe and easy to operate
- Overt or covert – Can be mounted inside or outside
- Clear 4-digit numbers – Simple

VERSATILITY OF ELECTRONIC

- Trucks - pedal runs
- With multiple doors
- Road tankers
- Airlines
- Shipping containers
- Brief cases
- Diplomatic bags
- Roll cages and drums

We can link our seals into any on/off switch, air pressure, open door, and a variety of tamper devices.

Pull type seals are small, put on bags.
Nanoseal can be fitted onto a cage.

NEW DEVELOPMENTS

- Automatic remote interrogations- next stage

On a truck we have a number of developments with RF manufacturing using their technology. Automatic Seal Verification Barrier raised when all checks OK

- Linking with other equipment
  - OVC versus 232/485
    - Refrigerator Units - We can transfer information on temperature
  - GSM – When this is open it will send signal in device. Global satellite signal
  - Satellite tracking – real-time, where it was when it was opened
- GPS position recording of opening and closings – Global Position Signal

Low Orbit Satellite Communications – Not available yet

FUTURE DEVELOPMENTS

- Microseal RS232/485
  - Multi input sensing – Separate seal number for each point, time and date for each point, download the information and talk to it.

Instead of having a single electronic seal which can seal just one point, we have one seal that can seal multiple points, generate separate seal numbers for each point, time, and date memory for each date.

Mike Farrar: What is the battery life?
Answer: 5 to 6 years. Depends how the battery is drawn down.

FUTURE DEVELOPMENTS (continued)

- Nanoseal – Sealing lottery bags in Spain, if the tickets aren't sold, our device will time and date, double the sales, midweek lottery
- Incorporating RF read write tagging with multi readability

READ WRITE SEAL TAG

- Identifies ID of bag box container
- Verifies seal integrity time, etc.
- Identifies content code
- Shipper owner sender
- Destination

CUSTOMER DEMAND

- Closed loop operations reusable – For tracking
- One time user RF seals – You might want to track even though it won't come back
- Price reflects volume

We have the technology, you have the demand. It all comes down to the amount of money. We have been in business 15 years, the customers just need to let us know what they want.

Jeff Miller: There is a lot of talk of money, have you done a cost analysis? And if so, can you show us the benefit?
Answer: Yes, it is a question of the cost of the mechanical seal you are using and how often you use them. The more you are using the electronic seal the cost of electronic seal goes down. It is free sealing until then and then you have to buy more batteries. This doesn't include management cost or logistics ours are not locks.

Bruce Roberts: We also have samples, walk out with your very own seal.

Question: What happens when memory is full?
Answer: It can contain the last 50, if 51 pops in, the first will be erased.

INTEGRATING SECURITY SEALS AND RFID TECHNOLOGY

Panel Discussion/Presentation
Moderator: Ron Gilbert, Pacific Northwest National Laboratories
Panelist: Simon Fiera, Encrypta Electronics LTD
Panelist: William Blasdell, SAVI Technology
Panelist: Donald Ferguson, Kasten Chase, Canada

On going project at Pacific Northwest National Laboratories – We are a Government research and development laboratory so we are not out there doing the commercial development.

- Internal intelligent buildings LDRD project – Working on RF technology to replace conventional wiring, retro fit buildings, smoke detectors, light switches etc
- Radio frequency tagging of honeybees – Project for DARPA, tiny tags on honeybees and monitoring them. Train bees to find other things then honey (i.e., TNT landmines)
- Dog tag with hand held reader – Doing with Navy, Air Medical Research Laboratory, replace dog tag with memory tag, history of information, hand held with a range of 10 feet GPS is on it and will relay to a central unit.
- Arms Room Inventory Tag – Doing for Logistics Integration Agency (LIA), tagging small arms, night vision goggles to detect tampering. Passive tag.
- Navy Inventory Tag – General Dynamics to tag larger items in a Naval shipyard.
- Predictive Technology – Rocket motor tag - Linked to a suite of sensors to monitor different items, temperature, and humidity of rocket motors,
- Nuclear Reactor Remote Monitoring Tag – Tied into the first, low cost RF tag with remote tag to monitor temperature, vibration, pressure, etc.
- Special Forces Locator Tag – New technology, find direction you can determine the distance
- Classified projects for the intelligence community

This is the work we are doing at Pacific Northwest National Laboratory and I would like to open the floor to the other gentlemen.

Panelist: Simon Fiera
Encrypta Electronics Ltd.

We pioneered and developed the original electronic seal technology 15 years ago. Since then the demands from industry has gone from a simple electronic seal to an intelligent memory and download capability. Primarily we used and still use infrared technology. This gives us compatibility across equipment, driving component cost down, and with improved performance. It is widely used on laptops, printers, etc. Effectively the button pushing can be eliminated by going to the RFID in industry, this saves time and money.

Like the early days of infrared, no standards were in place. We work with companies producing RFID and readers. RFID seems to be the solution looking for the problem. Different

applications require different solutions. Our truck seal has two-way read/write capability distance, every time the truck passes a read point the signal is recorded. The reader interrogates the seal, great tracking. With two-way communication we can send instructions to the seal now. Such as synchronize the times and dates, or change its operating parameters. We have interrogated RFID tags with different frequencies to suit different situations. Everybody wants the low price RFID tag but there are technical challenges that need to be overcome. The tag is battery powered (this makes the design and outside parameters critical), the antenna may cause problems. It is critical and in our case at the back of a truck in a metal box seems almost impossible. Solutions can easily be achieved but not the price.

- Data transmission - Must be secure and reliable, transmit the data quickly. In industry time is money.
- The memory size is large and on a truck must be transmittable quickly, we will continue to apply the RF technology.

Panelist: William Blasdell
SAVI Technology

One of the suppliers to Susian Vickers program for the general AIT and RFID programs.

What is Automatic Identification Technology (AIT)? – AIT includes a broad array of electronic tools which capture and transfer data about Resource at rest or In Motion.

- Bar codes
- Laser cards
- Smart cards
- Active tags – My focus, because this is what we are primarily involved in
- Passive tags

RFID tags are small electronic radio transponders which identify and track assets. RFID tags range from the electronic equivalent of a barcode to sophisticated micro-computers with two-way radios.

There are three types of tags:

- Inductive - The tag transmitter is energize in the radio frequency field generated by the interrogator.
- Back Scatter – The tag antenna reflects a small portion of the signal transmitted by the interrogator.
- Active two-way – Two-way communications and data transfer occur between the tag and the interrogator.

GREAT TECHNOLOGY, BUT LIMITED PENETRATION

- Lack of standards

- Hard to install (complex)
- Fact versus fiction

RANGE OF RFID APPLICATIONS- SOME OF THE APPLICATIONS WE SEE

- Electronic Article Surveillance (EAS) – the one you see in department stores
- Physical Security - Electronic Access Control
- Anti-Counterfeit (Knock-offs) – Low cost
- Asset Tracking (Security, Manufacturing, Distribution, Travel) – SAVI's interest in tagging containers in DoD markets
- Warehouse Inventory Control
- Shipping Container Tracking
- Pallet Tracking – US Post Office
- Yard Management (Transportation Distribution Center) – Vehicles coming into the facility

SAVI HISTORY

1989 Incorporated in Palo Alto, California
1991 Largest SBIR Phase II Contract
1993 First major installation (tracking Army shipments in Europe)
1994 Microcircuit Technology in Logistics Applications (MITLA) Contract SBIR Technology of the year by White House Office of Science and Technology
1995 Wholly owned Texas Instrument Subsidiary – Cornerstone of TI Asset Management Strategy which included TIRIS &TI Software
1996 Small Business Administration's Tibbets Grand Award for Outstanding Technology Operational Deployments in Haiti, Somalia, Bosnia, Kelly AFB and Cherry Point Naval Depot Operational Deployment, and US Army Medical Hospital Operational Deployment
1997 Toyota Operational Deployment Wholly owned Raytheon subsidiary USPS Pilot Program Operational Deployment to Track DoD Ammunition World-Wide Raytheon Management Agrees to Sell SAVI

Presently – We are a stand alone company
The following are the types of products we offer:

ACTIVE RFID HARDWARE

- SaviTag 410 – Read range of 300 to600 feet
- SaviReader 410R
- GateReader 410R- Narrow beam capability so that you can track only those vehicles that are coming in or out of a facility.
- MobileReader 410R
- Docking station – For loading tag information without RF.

A lot of these requirements came about because of the Persian Gulf War. We needed to identify what was inside the containers. About 98 percent of the equipment moving in to support the Kosovo operations so we have good coverage of equipment in the containers moving into those operations. We tag equipment and we provide computer systems so all can be reported back to the central site server. There is a web site, so that the company commanders can see where their equipment is along the route.

AMMO AIT/AIS INTEGRATION – One of the applications we are involved in. We found out that our company strategy is to be systems software solutions provider. Start out with our own products and work toward a third party product. Our goal is to provide the infrastructure that allows the people to use the tags and readers appropriately to their application. We have organized our business into standard products, then there is a professional business that takes our process in Crane, Indiana, primary depot all work is done on computers today eliminating all paper work. We track coming in, track going to ship. This is an ongoing program, this year six sites, next year double that involvement.

THE SAVI ARCHITECTURE - This is a three tier architecture, bottom our tags and readers, SAVI universal, SAVI Asset Manager (SAM), collects data and reporting, RFID network management, common application logistics and algorithms. Our goal is to make SAM a wide variety provider.

Lock tag system for commercial trucking

Origin Gate	Destination Gate
• Read Guard ID, driver ID, seal ID • Issue lock command • Write tag data • Generate reports	• Read seal ID, guard ID, drive ID • Verify tag and ID date • If OK, issue unlock command • Do not lock if not OK • Generate reports

We are not in the security business per-say, we are in the RFID business looking for applications in a commercial world or the DoD environment.

Panelist: Donald Ferguson
Kasten Chase, Canada

CORPORATE OVERVIEW – Kasten Chase

Who we are –deeply developing technology for customers. We are a communication company helping a wide range of products.

Our corporate technology - When access to real-time information is crucial, Kasten Chase's communications solutions deliver the right information at the right time to ensure professionals can make sound decisions on the spot.

CORE TECHNOLOGICAL COMPETENCIES:

- Internet Protocol (IP) connectivity
- Remote Access
- Secure Communications
- Network Management
- Wireless Communications

OPERATIONAL BUSINESS STRUCTURE

- Web-to-Host (Versa*Path*)
- Secure Remote Access
- Wireless Communications
  - Wireless networking (CBTC)
  - Radio Frequency Identification
  - Communication Management (InterTalk)

RFID - LINE OF BUSINESS

- Engineering Service Organization
- Business focus
  - Postal Market
  - Logistics Market
- Providing RFID solutions to solve customer problems

RFID RESEARCH AND DEVELOPMENT

- Expertise –
  - Development of robust Active and Passive tag technology for specific market applications and customers
  - Hardware Specific - Low Power RF enabling technologies

- Radio Location
- Manufacturing Product Support
  - RF specific product

QUALITY SYSTEM

- ISO9001 certified – Annual audits
- Last audit Aug 1998
- Surveillance Audits – Semi-annually

Market Model - We work with the system integrators and to the end customers throughout the entire process

- End users – IPC Domestic Post Office
- System integrators
- Lyngso Industries (Denmark)
- Siemens Electo-Com (Dallas)
- RFID Product Suppliers
  - Allen Bradly Rockwell International- Milwaukee

DEVELOPMENT OF AN RFID TECHNOLOGY EXAMPLE

In 1994 we were approached by the Danish Post with a compelling need for a technology to solve a specific problem.

- The problem that needed to be solved was that they need to prove to the people of Denmark that the Danish Post was providing good service and was continuing to make improvements in their Quality of Service.

TECHNOLOGY EXAMPLE

- The Danish Post had a vision
  - To use RFID technology in an Automatic Mail Quality Measure System to provide:
    - A transparent means of measuring the Quality of Service throughout the Post Office
    - A diagnostic tool to facilitate improvements in processing
    - Use it as a public persuasion tool to sway public opinion in their favor

TAG DESIGN CRITERIA

- Multiple read capability
- Must survive the riggers of mail sorting
- Must pass as first class mail – Weigh no more than 12 grams

- Must be read while in a metal cage moving up to speeds of 5 meters per second
- Must co-exist with other low power radio communication technologies
- Must be approved for use across Europe and North America
- Must have a service life of more than 4 years

READER DESIGN CRITERIA

- Common interface
- Internal time clock
- Memory buffer – Turn off or on and still store data
- Flexible software programming features
- Software upgradeable online
- Antenna diversity
- I/O for controlling external devices – Turning on lights and audible alarms
- Self diagnostics and supervision, addressable - If equipment went down then they could send someone over.

RESULTS

- We developed a line of RFID technology products specifically designed for the postal industry
- T95 postal tag – flexible devise
  - Flexible
  - Weight less than 12 gms
  - Fits in a regular envelope
  - Excitation range over 5 meters
  - Read range over 25 meters
- R95 reader system –
  - Robust enclosure
  - Compatible with reader infrastructure
  - Easy to install
  - 10 year life 5 year battery life and has a replaceable battery
  - Can be programmed inductively

As a result of the Danish initiative we have International use

- 20 countries including – United Kingdom, France, Germany, Italy, Spain, Portugal, Greece, Denmark, Sweden, Norway, Finland, Holland, Ireland, Canada, U.S., Austria, Switzerland, Iceland, Luxembourg, and Belgium

DOMESTIC USE

- Denmark, Ireland, Norway, and Austria, for quality of service

SYSTEM STRUCTURE

Local area network (LAN) or external private/public network international applications data sent

INTEGRATING SECURITY SEALS AND RFID TECHNOLOGY

- RFID technology can be classified as:
  - An enabling technology
  - A gin and tonic technology. With every gin and tonic technology you consume you can usually think of another application where the technology can be used.
- Assume all the necessary market reasons for integrating security seals and RFID Technology exist (i.e., a customer exists with a compelling reason and the money to buy the product)

OBSTACLES

- Each application is typically unique requiring a specific solution.
- The product is considered a commodity item by the customer.
- Competing technologies are very low cost.

One RFID product will not solve everyone's problems.

TECHNOLOGY OPTIONS

- Passive and/or active
- Each electronic seal application is unique and will dictate future tags

FACTORS EFFECTING THE TECHNOLOGY DECISION

- Range
- Cost and volume

FACTORS THAT SHOULD BE CONSIDER IN THE DESIGN PROCESS

- Ease of installation – If it is not easy to install the customer will be unlikely to buy it
- Ease of use - Customer friendly
- Radio approvals global or regional use – Big issue
- Program flexibility flash memory – When you develop new technology the more flexible the better
- Co-existence with other intentional radiators
- Reliability environmental considerations
- Security
- Power requirements

IN TERMS OF ACTUALLY PROVIDING SOLUTIONS

- We are currently working the electronic seal providers on new product.
- Under current NDA I am not allowed to disclose any technical details at this time.

Question: (for Bill Blasdell) On your units when you program, how do you load? **Answer:** You can use a docking station, hard wired to the tag, through the integrity, it is not encrypted.

Question: How do you manage the program, who has access to change, can it have the parameter changed, can I override it?
Answer: The tag is burned in the factory. The program can't be changed, the data can if you have read-write technology.

Question: Have you considered password protection, and does it have a real-time clock so that if things are changed it is documented?
Answer: Yes, time, date, stamp in the integration, tag does not have real-time clock. The time/date, that is a concern.

Roger Johnston: Contrast between RFID or infrared depends on number of times of operation. Our units have both infrared and tagging.

Mark Hayward: Just a comment for the panel. We may not get to a generic tag, yet SAVI has a generic tag. It concerns me that if there is never going to be a generic tag every application is unique, the chance of getting this into the market place may never happen and I am wondering if we will only end up with a generic tag.

Answer: I think the trend will be to standardize the communication link. In terms of the encrypted seal, the direction that would be taken with any seal is there will be a standardization of the communication link and possible protocols in the command at the API interface at the software level. Once you standardize, the form factors will vary from seal to seal, but the communication link will move toward the standard.

Mark Hayward: I meant in the terms of foreign factor. There will be customization, case-by-case, a foundation that will also have deviations to address your customers needs.

Bill Blasdell: I think that you will find out that in a few years there will be different devices at different kHz, and a set of suppliers, applications with standards, we are not there yet. There is no standardization today, but to be a viable supplier our approach has been we are going to do the integration at the computer system level, we can be economically viable until such standards are here.

Don Ferguson: There is a draft of an ANSI Standard available on the web which defines the applications interface at the software level. There is some detail as to the RF protocol, etc. This is on the internet and it is a draft.

ACTIVE TAG AND SEAL TECHNOLOGIES DESIGNED FOR THE UNATTENDED MONITORING OF STORED NUCLEAR MATERIALS

Chris Picket
Oak Ridge National Laboratory
Oak Ridge, TN

THE Y-12 ORSENS PROGRAM

- Consists of several systems and technologies all designed with the purpose of making the Y-12 Material Inventory Process:
  - Safer – Eliminates radiation exposure to personnel
  - Faster – Inventory available on demand
  - Cheaper – Significantly less labor, less training, two-person rule
  - 100 percent - Sampling schemes not needed
  - More secure – Individual item surveillance on each item. This gave us inventory extension credits with DOE
  - Adaptable – A variety of materials and storage environments
- Continuous Automated Vault Inventory System (CAVIS) – Radiation and weight measurement system monitoring on stored items
- SmartShelf - Automated item tracking system active tag technology – Inventory system using electronic tags to identify unique containers, authorized users and storage sites.
- During an emergency, that would be a time to advert, involves swat teams with wands and hand-helld scanners. Have a real-time inventory. Give information when, what, and how long it has been gone from the location
- Movement of containers is automatically logged by the system

SmartShelf is an electronic tag system that we can attach to each container. Basically have a real-time ID tag. Where barcode labels are easy to forge, these are tamper-proof. Main components, beside the unique tag - node computer - from that we have a cord from the container that can pull 200 to 500 items. This can extend our system that feeds into our main data base.

SmartShelf ID buttons – another component, unique ID tags. We have a protocol. Present a Node box, 10 to 15 seconds to attach the item to the network. If an alarm does not go off, then everything is OK and they can go about their business. We use this with a two-person rule.

The assembly of these boxes in the production area is more labor intense then we wanted. Mounted in two steps, first the box, then the cover. The other box can be mounted with the cover on. It saves on installation in the field.

DIFFERENT WAYS TO ATTACH

- Touch memory
- Attachment plate

This is an accountability system more than a security system. Because we live in a world of barcodes, we have made the system work with the barcode systems. The buttons have memory, currently we have some containers that have more than one item per container, this tag you can wand barcodes. It reads buttons. A container that has several items, we swipe the new barcode and write it to the button by touching the button. Successful techniques.

OPERATIONS

This technology was also sent to Russia, we were having some problems, part was communications, it happened to do with Microsoft Access in the data base. The difference was between the U.S. date formats and the European date formats. Problem was solved.

CAVIS IN RUSSIA

They ran it through several environmental conditions, only problem we discovered was when it got 190°F, the wire needed to be replaced. Then it functioned properly.

REFLECTOACTIVE SEAL SYSTEM

- Four major components.
  - Optical signals. We send light through a fiber optic connector, connected to a container, it monitors a seal breach and location, therefore, we can also tell which seal is breached. It is interfaced with a two man rule.
    - Authorized
    - Registered
    - Performed

Different modulation, physical protection some required.

- Resist dense storage
- Monitor with one system 1,500 to 2,000 items.
- Tracks time when seal is breached
- Seals are reusable, open and closed according to the manufacturer 1,000 times, any where you attach a passive seal or lock you can use this system.

It is continuously monitored which cuts down on seal inspections and extends our inventory time, based on our inventory.

The way it works, look down the cable, both directions, open is larger bi-directional breach detection. Gives a very specific location. Thresholds are set, alarm levels and warning levels, wasn't attached properly or was damaged or dirty.

We gave sensor system and information systems.

GraFIC – Graphical Facility Information Center design to do specific things.

WHAT IS GraFIC

- An information system which allows for fast confirmation of the inventory status of stored items
- Works with sensor subsystems to provide user interface and long-term data storage
- Creates alarms to notify the users of system problems, such as out-of-limit sensor readings
- Offers information which aids in problem resolution
- Provides intelligent facility management features

BACKGROUND

- One of the Y-12 Plant's major missions is Special Nuclear Material (SNM) storage
- DOE Orders require that SNM inventories be confirmed periodically
- Inventories provide assurance that the SNM is secure and has not changed
- Currently, these inventories involve manual measurement of weight and radiation levels

Starts with a different devices on the floor plug and play

- Sensor concentrator three classes of sensors we can monitor with this system
  - Highest level is the smart sensor – A sensor that has intelligence on it
  - Hybrid - Where you can program the sensor to do certain things
  - Third is dumb sensor - Like a thermocouple that can be attached.

GOALS FOR GraFIC

- Less expensive (fewer people involved)
- Faster (at the click of a mouse)
- More secure (no manual access required)
- Safer (no potential radiation exposure)

WIDE APPLICATION

- The features provided by GraFIC would be useful in other facility/inventory situations
- GraFIC is designed for ease of interface with various sensor subsystems and storage configurations
- Intelligent facility management (IFM) features are being provided which have broad application

CURRENT ACTIVITY

- A new version which will handle any hierarchical storage configuration is being developed.
  - User-entered storage configuration properties
  - User-entered sensor subsystem properties
- Adding interface to Y-12 SNM accountability database

GraFIC COMPONENTS

- **Sensor Subsystem –** Monitors sensors and provides short-team data storage
- **Sensor Polling and Configuration System (SPCS) –** Front-end processor which communicates with one or more sensor subsystems and provides medium-term data storage
- **Database Server (DBS) –** Communicates with one or more SPCSs and provides long-term data storage in relational database
- **Workstation –** Provides user interface

Typical layout, boxes are monitored and attached to a computer that is protected in a computer room, two system added redundancy.

TWO TYPES OF USER INTERFACES THAT ARE BUILT INTO THE INTERFACE.

STANDARD VERSUSCUSTOM

- A standard user interface is provided which will work with any hierarchical storage configuration – Resembles window explorer
- Custom windows may be added (at added cost) to provide a storage configuration – aware view of the system status

STORAGE EXPLORER

- The standard Storage Explorer provides a hierarchical view of system configuration and status
- Details may be requested
- Custom interface is a mapping interface – We start with a map of the world, click on the site map and you can see we color code buildings, click on building and see plan

STACK AND MSV STATUS

- The custom Stack Information window gives the status of each vault in an MSV stack
- The custom MSV Information window reveals status or each cell and sensor within a vault

We keep 30 days on the system before we dump it into an archive.

FACILITY DRAWING

From this standard window you can:

- View storage status
- Position icons
- Select lots for inventory reports
- Plan future storage
- View procedures

FIND

- Allows the user to search for assets, storage locations, alarms, etc.

EASY UPDATES

- GraFIC allows users to enter/update facility components, stored items, etc.
- Automated data entry from existing sources is available
- GraFIC provides context-sensitive online help to answer user's questions.

CREATE REPORTS

- Several predefined reports are provided.
- Our inventory reports we can be done on command.
- Reports may be viewed on-screen or printed.

Facility people wanted to deal with choosing a container, previously defined standard container, and define a new container, fill in ad-hoc dimensions manual and auto. The person sitting in their office would not have to leave.

SECURITY MEASURES

- Users are assigned roles which determine the GraFIC features they may access.
- A two-person rule is enforced for all configuration updates and for alarm acknowledgements.
- Windows NT provides security features such as file access control.
- Oracle Secure Network Services may be used to checksum and encrypt database requests and responses.

SUMMARY

- GraFIC was initially developed for use in the Y-12 plant for SNM inventories.
- GraFIC will fit other facility and inventory situations.
- GraFIC provides inventory confirmation, alarm notification, and facility management features.

For more information http://www.ornl.gov/orsens

Questions: What makes the button in the SmartShelf™ not vulnerable? Wouldn't it make it easy to counterfeit a chip and put in the system?
Answer: The serial number is in the inside. I'm not saying they can't, but we have to have it register at our system. The technology exists.

Question: Does the laser look at phase or applitude?
Answer: The laser looks at modulated frequency, Sutto level.

Susian Vickers: Just a little advertisement, the touch level button is already on the AIT II contract.

RADIO FREQUENCY TAGGING DEVELOPMENTS AT PACIFIC NORTHWEST NATIONAL LABORATORY (PNNL)

Ronald Gilbert
Pacific Northwest National Laboratories
Richland, WA

This is Part II, because I was here last year. New things this year:

- Commercial RF tags attach tag single chips systems tags, low cost, micro stamp engine module, silicone they want to sell tagging honey bees.

HOW DO THEY WORK?

Continuous Wave Backscatter Modulation- Not much energy, not a transmitter, some are battery powered

- Reader emits a "continuous" RF signal
- RF energy provides power to the tag
- Tag "modulates" a preprogrammed message
- Modulated signal is decoded by the reader

10 character ID tag, passive integrators, two-person code, read only – This is placed on honey bees. Very small.

RF BEE TAGGED DETECTION SYSTEM

- Three antenna coils
  - Bee arrives, detects entering and/or leaving, RF driver and decoder, sends signal to computer, decodes, wireless modem

You can have multiple decoders, time and date.

Question: How do they get attached?
Answer: Healthy dollop of epoxy. First they chill the bees for 4 minutes and then stick the tag on with epoxy. The smallest RF tag I've every seen.

GARMENT TAG SUCCESSFULLY DEMONSTRATED SEPTEMBER 1995

- Joint effort with Los Alamos National Laboratory (LANL), PNNL
- Features:
  - Read/write capability
  - Multiple tags in an RF field
  - Completely passive (no battery)

HIGH VALUE ITEM SECURITY SYSTEMS (HVISS) – DEVELOPED FOR THE ARMY

- >600 foot range (demonstrated)
- 32 bit ID code = over 4 billion tags
- Input monitoring capability
- Output control capability
- Final design will be “semi-passive”
- Great design for a “seal” tag.

Temperature, pressures, analog information. We can control the output, we can turn it on and off.

PROTOTYPE SEMI PASSIVE TAG - SECOND GENERATION

- Elliptically Polarized Phase II Antenna 1-inch by 0.4-inch – Night vision goggles, registers the name with that pair of goggles, high end items.

PHASE II TAG DIGITAL ELECTRONICS BOARD

- Battery powered
- Micro-controller based
- Input monitoring capability
  - Jumper Status - on/off
- Output control capability
  - LED - on/off
- Can be reduced in size

PHASE II 2450 MHZ PATCH ANTENNAS

- Two-dimensional design
- Linearly polarized
- Bi-Static
  - Separate antenna for
    - Transmit
    - Receive

PHASE II HAS DIGITAL COMMUNICATIONS AND GRAPHICS USER INTERFACE (GUI)

- Interrogator to Tag Communication Protocol Designed and Implements
- Digital Signal Processor uses PC audio port for input
- Visual Basic User Interface for Demonstration Purposes

LOW POWER ACTIVE TAG

- Cordless telephone technology. The idea was this had flash memory, leave tag out in the field until the right person could access this tag. Looking for a RF signal when it did it would power up the rest of the circuitry then look for an ID code, then it would "wake up and spill its guts." Could survive 2 years in the field.

ADVANCED SMART MULTI-SENSOR SYSTEMS

- Remote Read RFID Sensor Units
- S1 - Temperature
- S2 - Humidity
- S3
- S4
- S5

For inventory tracking. That way you could tell which ones you want to use and which ones you can't because of age.

Impact Test - Location A – As it ages the data will change.

ON-GOING PROJECTS AT PNNL

- Internal Intelligent Buildings Project
- Radio Frequency Tagging of Honeybees
- "Dog Tag" With Hand-Held Reader
- Arms Room Inventory Tag
- Navy Inventory Tag
- Predictive Technologies – Rocket Motor Tag
- Nuclear Reactor Remote Monitoring Tag
- "Special Forces" Locator Tag
- Classified Projects For The Intelligence Community

SUMMARY

Three categories of RFID Tags Under Development

- Fully Passive – No batteries
  Short range - <30 feet
  Low cost
  Simple
- Battery Powered Backscatter (Semi-Passive)
  10- to 500-foot-range (typical)
  Input monitoring and Output Control Capability
  Long battery life >5 years
- Active (full blown transceiver)

>500-foot-range
Multiple sensor suite of inputs
Micro-controller/neural network decision making capability
Short battery life (months)

POINTS OF CONTACT

Ron Gilbert
Phone 509-375-6672
Email: ron.gilbert@pnl.gov

Paul Sliva
Phone 509-376-7827
Email: paul.silva@pnl.gov

Curt Carrender
Phone: 509-372-4929
Email: Curtis.Carrender@pnl.gov

James Skorpik
Phone: 509-375-2168
Email: Jim.Skorpik@pnl.gov

I think as far as the National Laboratories go we have a system that is pretty good with good ideas. Just from going to conferences like this one I can tell there is a lot of need for tags like this. As an engineer and researcher in the National Lababoratories I don't know that much about the commercial development and what we need to do next, but I would sure be interested in talking to anybody here so that we can get it out for mass volume production.

Jim Crabtree: I presume that one of the sensors you could put in is Radiation Detection?
Answer: The tags have a micro you can use and detect a variety of interfaces. Photo multiplier you would have enough power to run a tag.

Jim Crabtree: Do you have any ideas how you would link one with pressure sensitive type seal, is that possible?
Answer: We haven't done much. Oscillating frequency.

Comment: In reference to the chips that turns on and off, how are you taking care of those devices?

Answer: All I know is that they are concerned with night vision goggles, they would be useless, turning things on and off, that is what they have asked for.

Eric Elkins: What is the process to disable those tags on the night vision goggles? **Answer:** Very simple, input and output control, a switch with on and off, we are tied into the on board electronic. So opening the switch you don't need that voltage.

Eric Elkins: Can I jump through that?

Answer: We can jump through as many hoops, you can have many levels, we can make the tamper-detection as complicated or as simple as you want.

TRAINING INSTALLATION AND INSPECTION PANEL

Panel Discussion/Presentation
Moderator: Mike Farrar, NFESC
Panelist: Anthony Garcia, Los Alamos National Laboratory
Panelist: Patrick Horton, Sandia National Laboratories
Panelist: Randy Cabeen, TRW

Mike Farrar: In our first symposium a gentleman from the customs office located in the Port of Los Angeles stated that there are 100,000 containers that come through there monthly. Of that amount 700 got looked at and of that 150 got a second glance.

What training do the inspectors have? None, very few people are trained to look at seals. I have been to shipping yards and I have seen seals cut off and thrown on the ground. I have seen boxes of seals open and sitting on the floor. We need to teach people on the proper applications, removal of them, handling them, how to control. Drivers were intentionally trying to break open the seals until they were made accountable for them. Train people on the proper use and control. The Navy used to send their less than average performers to security. Just to get rid of them. We need to train our people. Inspire people to do a good job. Inspection of seals, this is something we need to do.

Panelist: Tony Garcia
Los Alamos National Laboratory

SEALS TRAINING, INSTALLATION AND INSPECTION

We believe that effective training is crucial for:

- Effective installation and inspection
- Employee buy-in and positive attitude
- Reducing vulnerability during seal
  - Procurement
  - Storage
  - Checkout
  - Record keeping
  - Removal and disposal
  - Reporting and analysis

Principles of effective training (and an effective seals program):

- Treat the job as a time-honored and serious profession
- Treat security personnel as knowledgeable professionals
- Accept and acknowledge feedback
- Explain the reasons for required procedures

- Emphasize that security is mostly about paying attention
- Emphasize that security is not an absolute, it is about compromises
- Make training specific for your seals, application, and facility

These are controversial:

- Show seal installers and inspectors how to defeat the seals and containers
- Encourage them to think about how to attach the seals, containers and overall security program

Panelist: Patrick Horton
Sandia National Lab

As far as DOE is concerned seals are controlled on the way in and on the way out. The whole process from what I have seen is done quite well. I started 6 years ago. I sat in a re-training program for the seal applicators, that gave me a pretty good impression of how the business is done. If that is typical it is very well done. The DOE takes this very seriously. This will be more of an overview of what I have experienced in the six years. DOE uses seals in what is called a ***Layer of Protection***. It requires a badge to get on the ground (through the gate), limits access into controlled areas where the materials are stored and processed coming and going, armed guards, metal detectors, makes sure nothing is coming out. Very well planned ***Layer of Protection*** process. There is a two-person rule where the vaults and seals are utilized. Depends on the material that is being stored. Each DOE site runs its own program, depending on their own needs at their specific sites. I think it is a really good way of doing business, they meet the needs of DOE's requirements.

The Training Program - You should be trained on the actual seals you are using, any way that provides the best protection. The containers are used over and over again, make sure the surface is cleaned properly before new seals are used again.

Pressure sensitive seals are applied on the fruit can. A pressure sensitive seal then will run along the side, rotate, and do the same thing on the bottom to protect the top and the bottom. On paint cans the same type of process. (e.g., 1-, 5-gallon paint cans). Plastic jars are used as an interim storage process, not used on long term because the seals will not stay on them for long term. Examples 30 to 55 gallons storage drum, locking collar, cage rooms, monolithic wall storage doors.

Seal installation configuration threading of a twisted wire pier, 55-gallon has a locking collar that has an open hole, you run a bolt through the threaded stud, through and down, outside, some do single, a lot do the double configuration.

During inspection the configuration lends itself to a positive inspection. Inspectors like to do a walk through.

Example situation - Loop seal

- There is a facility that used a particular seal that required four parts. The vulnerabilities for tampering - they determined that a tool could be utilized to pull it through and cinch it up, the inspector could visually see that the loop seal could or had been tampered with.

During the inspection of the seals process by the inspectors is an integral part, train the applicators, inspectors are knowledgeable of the seal training, installation and inspection. My understanding at the DOE facilities the whole process is done very well and the records show that.

Panelist: Randy Cabeen
TRW

I am going to focus on one component and that is the forgotten role of the inspector. Often overlooked intentionally, I have been in training for over 10 years with Sandia INEEL, Oak Ridge and Pacific Northwest. I have also been involved in a system development with DTRA and involved testing with Sandia, LANL, and a variety of commercial vendors. I have a broad experience in this realm.

UNUSUAL USER INSPECTOR INVOLVEMENT

- The inspector/user is taken into serious consideration when:
  - The developer is considering if there is a market for a product
    - Considered, but not as much as the buying agent
- When you try to find a user/buyer for the product
  - As an avenue to finding a buying agent
- When the inspectors complain about the lack of usability of a product after it is forced down their throat
  - Usually only considered here when you are trying to get them to do what you want them to, not what they want or are suppose to do

THE INSPECTOR IN THE DEVELOPMENT CYCLE

- Definition of requirements for a product to be suitable in anticipated role(s)
  - Sometimes buyers have a tarnished vision of what inspectors do, if they have one at all
- Early Research and Development cycle
  - Iterative involvement during prototyping to identify needed modifications before production
- During product development

The most amazing thing is talking to people, have them explain to you what they need, then talking to an inspector (procuring is different) get to the inspectors early in the process. First, you find out the things that were missed at the end. Keeping the inspectors in the loop helps immensely.

What are the operational procedures, how do I use this? It is rare to see the details on inspection procedures. Use common sense, talk to people.

THE INSPECTOR IN THE ADVERSARIAL ANALYSIS PROCESS

- Adversarial analysis often does not even consider the inspector
- Actual operational environment of the inspector (primitive working conditions, short timelines, etc.) is often neglected.
- Training of inspectors is usually conducted post adversarial analysis if at all – often the ones used are the adversary? Rarely trained with the user.
- Need to train inspectors in distinguishing between tampering from normal "wear and tear."

You will be surprise how easily people can figure this out. One thing we tend to do is we put simulated tamper and simulated damage. It forces the inspector to take a different look. Inspectors sometimes are "new" or "green." Identify the difference of tampering versus wear and tear.

The avenue or range of inspectors we have had range from privates and full colonels, variety of countries, education from GRD, up to Ph.D., and what we have notice is that there isn't much difference. We have notice that Ph.Ds., are usually the worst inspectors. That is the trend that we have seen. Also, with inspectors, in every test regardless of experience or age, there is a challenge of trying again. Go through initial training, they put the items on inferior. Your first items you put out in the field will be inferior.

BUYERS OFTEN FORGET THE INSPECTION

- Lacking inspector input, buyer may unwittingly accept a product whose features poorly match actual requirements.
- The ultimately high cost of minimizing training expenses:
  - Inspectors less effective until experience gained
  - Heightened possibility of security compromise while inspector is learning on the job.
  -

Why are you are trying to minimize your key link?

SIMPLE INSPECTION

- Three systems that were defeated, two were defeated and forced hundreds of dollars of re-engineering. All three with junior engineers found every single item that defeated them. They defined and explained the process. Re-engineering.
- Listen to the inspectors. Keep the inspectors in the loop, work and include them as part of the security system.

Kim Rasmussen: We have heard the word "defeated" used multiple times in the past two days and in different context. What is your definition of "defeated" in respect to security seals when the word "defeated" is being used?

Answer (Tony Garcia): For us the seal has been opened and put together without any indication.

Roger Johnston: We define it as gaining entry with or without damaging the seal or with or without creating evidence of entry and then resealing accompanied with one of the following, if necessary. Repairing the damage, if any, and replace entire seal or parts with a counterfeit, but the bottom line is you can fool the seal inspector.

CLOSING REMARKS –
Eric Elkins, NFESC

We have brought people together in this community from a very broad range of technology. But, I was very entertained for the last two days. I wrote down my thoughts of the conference.

I think what you gain is more than dollars, you gain and learn about technology. The mixture between Government and industry, I hope you got a better understanding of what the Government needs and things you can do to help us with seals technology. From the Government side we can help develop technology by letting you know what you need. The goal of this conference is technology exchange. I would like to compliment everyone, you did an outstanding job. I know it takes along time to prepare for this and we certainly appreciate it.

As far as technology advances, Ron Gilbert's presentation certainly showed that since the last conference his product alone, the technology has changed. To follow Rogers comment it looks like we want to know if anyone is tampering with our stuff.

One of the benefits of these meetings is to establish relationships with people in other businesses, get to know people in the Government, what their needs are and visa versa. I think the products, technologies, and services that have potential to solve the problems that we have, and I hope others have seen the same thing. We can look at improving security and help keep the cost down.

One of the points I wanted to bring up is, I would like to see a show of hands, are you still interested in us in sponsoring another symposium in 18 months or less? Everyone raised their hand. Good, outstanding. We will enjoy receiving your comments. I'm sure that if I told my sponsor that we wanted to hold this once a year, and had the turn out that we had I am sure we could accommodate that. Other than that I would like to thank you for attending and I hope you have a safe trip home.

Bruce Roberts (Encrypta)**:** Thank you Eric, and if anyone is interest in having any information of the National Cargo Security Council I do have extra copies here.

Eric Elkins: I would also like to thank Bart, Jane, Barbara, and Jaime for all of their help, a class act.

ACRONYMS

AIT	Automatic Identification Technology
ASD	Assistant Secretary of Defense
ASTM	American Society for Testing and Materials
BSI	British Standards Institute
CCB	Configuration Control Boards
CID	Commercial Item Descriptions
COPO	Central Ordering Processing Office
DBS	Database Server
DISC	Defense Industrial Supply Center
DLA	Defense Logistics Agency
DoD	Department of Defense
DSP	Defense Standardization Program
DTRA	Defense Threat Reduction Agency
EAS	Electronic Article Surveillance
ECP	Engineering Change Proposals
ERP	Enterprise Resource Planning
ESC	Engineering Service Center
HNA	Host Nation Approval
HVISS	High Value Item Security Systems
IFM	Intelligent Facility Management
ISMA	International Seal Manufacturers Association
LANL	Los Alamos National Labs
LIA	Logistics Integration Agency
MITLA	Micro Circuit Technology and Logistics Applications
NCSC	National Cargo Security Council
NFESC	Naval Facilities Engineering Service Center
NGS	Non-Government Standard
OAS	OneSeal Automated System
OTS	OneSeal Transponder System
PNNL	Pacific Northwest National Laboratories
POD	Proof of Delivery
RFID	Radio Frequency Identification Device
SIR	Sensor Information Relay
SNM	Special Nuclear Material
SPCS	Sensor Polling and Configuration System
STAMIS	Standard Army Management Information System
TID	Tamper-Indicating Device
UL	Underwriters Limited

SYMPOSIUM QUESTIONNAIRE

SUMMARY OF RESPONSES TO QUESTIONNAIRES — 27 RESPONSES RECEIVED

1. Should the DoD Lock Program continue to sponsor this type of Symposium for Security Seals, TID's, and RFID in the future? Yes = 26 No = 0 No Response = 1.

One Comment: Definitely, but other departments could be involved further.

Please tell us why you feel this way.

- Experience, good knowledge of users and vendors. ◆ Unique forum.
- The exchange of information is valuable to Government and industry.
- This is the only forum available where idea and product concepts can be shared.
- Off-line communication; networking; continued education.
- Good forum for information exchange between vendors and Government.
- It seems that systems are gaining political support.
- With treaty efforts, non-proliferation issues, programs like this encourage the commercial sector to participate.
- It is the only forum available to become acquainted with these technologies.
- It was very valuable to me.
- New applications and requirements are constantly materializing and the people involved would benefit from this symposium.
- This is a good way for Government to keep track of seal technology; interface with Government.
- I don't believe there is another forum that is addressing these issues. It makes a great opportunity for DoD to communicate with industry.
- Great method of bringing together varied entities of technologists, users as well as providers together. This is very hard to do without this type of medium!
- Excellent opportunity for Government and commercial to get together.
- The Navy, my employer, has problems with defining requirements and then defining how to meet the requirements. We need to have a unified approach for the fleet users then fix our documentation.
- Security Seals, TID's and RFID's will continue to be important to National security and DoD. The conference provides a good method for exchanging information between DoD, other Federal Agencies, and private industry.
- The exchange of ideas between people and agencies having common interests — and otherwise — would not have reason to be together is very special.
- Valuable exchange of information about seal programs and technologies.
- DoD needs are not always what other users require.
- This is an important area of technology with lots of future promise.
- We need more dialogue/interfaces with DoD, not less. How about the industry sharing the sponsorship and getting together more often?
- The information about seal usage and technological advances is invaluable and would be difficult to obtain in another method.
- Provides a needed forum where users communicate, and interact, with vendors — and vice versa. RFID is the way of the future.

If so, how often should it be held?

Each year? = 13. Every 18 months? = 11. Every 2 years? = 6. Other? = 0.

If Government funding was not available to subsidize the Symposium, would you be willing to pay a $500-$600 Registration fee?

Yes = 13. No = 12. Any suggestions? (Editor's Note: None were offered.)

2. **Do you like the Symposium as it is now structured?** Yes = 25. No = 0. No Entry = 2.

What would you suggest for improving the structure of the Symposium? (i.e., separate workshops reporting back to the main group, increased or decreased panels, etc.)

- The panels are good. ◆ No, keep the present structure.
- Facility tour. ◆ No change
- Extend it to three days to include more papers.
- It's excellent the way it is.
- Less vendor pitches, more technical information..
- Newsletters, e-mail, and other mailings should be sent to participants between symposiums. We need to pursue these issues between symposiums.
- I don't see a need to separate now. If the scope increased the one area that could be split out is the shipping container topic.
- The whole symposium is small enough to keep everyone together. If it doubles in size, maybe split into groups. Also, invite some ex-military who are now in commercial security. I.e., Compaq, IBM, etc. Use ASIS members' directory for mailing.
- It would be great if it could somehow be compartmentalized so that the attendees could concentrate on areas that are of specific interest to them.
- I think the format has matured and doesn't require much change.
- Separate workshops to work the issues and progress toward solutions. DoD must take advantage of the expertise available in the other specialities to move forward. Demonstration projects, development of standards, policy, and guidelines is a must.
- I would prefer less commercialized self-serving speeches. Tuesday was great — Wednesday not as great. (Editors' note: We continue to request that presentations cover seal technology topics and issues. We ask presenters to avoid marketing "pitches" that do not provide technology transfer or are not of interest to a majority of attendees. Unfortunately a few speakers have taken advantage of our platform to "hype" their products.)
- Somehow, the Navy must get its act together and define what we propose. Then the Navy must resolve its requirements at the DoD level for compatibility purposes.
- Splinter groups/workshops would be a good idea.
- Separate workshops reporting back to the main group would be good. The composition of each group would ideally be composed of industry and Government representatives.
- No recommendations at Present!

3. What did you like best about this symposium?

- The focus on RFID. Good Keynote Presentation from Richard Williams. Would like more of these to help vendors focus.
- New technology and new ideas.
- The exchange of seal technology ideas.
- Technology updating — Keynote Speaker — Off-line communications
- Panels, variety of presentations.
- Good mix of vendors and Government officials.
- The freedom of information flowing between participants.
- The selection of papers.
- The product and participant diversity.
- It was very informative. I actually met people, and firms, in the field that I didn't know existed or did this type of work.
- The size and mix of industry and Government.
- Presentations by Dr. Johnson and John Tichenor.
- The opportunity to see what is going on in the community. The ability to interact between users and vendors.
- The varied demonstrations and availability of the users to discuss requirements.
- Mix of people.
- The interaction of all people. Many opportunities to mingle, present ideas. And I like the Mandalay (Embassy Suites Resort) as a location.
- First, the opportunity to see the current state of the industry regarding hardware. Second, the chance to talk to the Navy personnel about where the Navy is and where the Navy is going.
- Richard Williams was a dynamic speaker. I liked the displays. I was appreciative of the knowledge I was able to obtain. Dr. Johnson's insight into tags/TID's was great.
- Richard Williams — Roger Johnston — Ronald Gilbert.
- Talks about new technologies.
- The discussion about how seals supplement security, they do not act as the entire security program. Presentations form the Los Alamos group.
- Very well coordinated — Bart Hanchett does an excellent job of planning, Nice location! Plenty of lengthy breaks.
- The interface between Government (requirements) and manufacturers.
- Sharing of technology.
- The information provided by the true experts in the field and manufacturers.\
- Agenda, location, speakers.
- The people and the information.

4. What did you like least about this symposium?

- Nothing really — All was well. ◆ Nothing comes to mind. ◆ All good. ◆ Nothing.
- Hard to identify — Liked it all. ◆ Nothing, it was all good. ◆ N/A (3 responses).
- Nothing — Very well done. ◆ Not having all the Navy players in attendance.
- Scope of presentations was supposed to be noncommercial which was not honored by a vendor of electronic seals. Lack of Government personnel responsible for issuing guidelines.

- Having to sit in a room all day so close to the beach.
- It did not address problems the DoD community has with replacement of lead seals, nor did it review the history of what was done and who decided lead should be eliminated. The Navy has many problems with replacing lead seals on conventional ammunition containers and since the Navy (NFESC) seems to have the lead on seals, this should have been brought up.
- Not having the LCD projector until the last minute screwed up our presentation opportunity. No commercial users.
- The panel presentations were (for the most part) too long. After being verbally abused it is hard to focus on asking questions. Presentations were more like sales pitches than informational exchanges. I don't feel they were focused on the subject topics as well as they could have been.
- Amount of free time during breaks to converse with others attending the symposium.
- Not all seal companies (as vendors) were here — How were the people chosen? Advantage from back east was not here.
- The amount of marketing from the vendors and especially the Government speakers.
- Panel discussions. Less papers that are "sales pitches" from vendors (focus on technology and applications), e.g., more issue/need papers.
- Having two days midweek instead of at the beginning or end of the week is more disruptive to getting work done back in the office.
- Vendors on the panel who "answered" questions by telling about their products. The questions asked were never really answered.
- Lack of user discussion to identify needs. I think separate working group meetings of Government only personnel would facilitate forward movement of technology to applications.
- Product endorsements by the manufacturers who have an obvious interest.

5. We have had suggestions to extend this Symposium to 2½ days and include equipment demonstrations and testing. Unfortunately we were not able to find an organization that would provide hands-on demonstrations for this Symposium. If you do testing, would you provide a demonstration of your techniques at future Symposiums? Do you have any suggestions concerning demonstrations? What types of demonstrations would you like to see?

- Exhibit of tampered seals. ◆ RF and IR systems. ◆ No.
- Workshop on how to apply, remove seals. How to tell if tampered Literature covering these areas.
- Types and methods used by National Labs to test seals and other equipment.
- Yes, on test procedures and training.
- Testing can be classified or proprietary. Demonstrations can be furnished. (Consider a poster session.)
- RE: Type of demos: Practical, field conditions demos.
- It would be good to have a vendor "show and tell" at the meeting. Not only vendors, but also DOE and DoD labs.
- I would like to see demonstrations of techniques to defeat seals.
- I think the idea is good — would like for Los Alamos to show us their techniques.

- A ½ day vendor show and tell would give meeting participants more time to check out hardware and to become familiar with technologies in a "hands-on" manner. Maybe DoD or DOE could sponsor the extra ½ day.
- We provided live demonstrations at this symposium through the contract prime. If you would like an application-specific type demonstration, please contact me - Susian Vickers, PM AIT.
- My activity does not perform testing on seals but I would be interested in such a demo, even if it were on video.
- We do testing but as of how it is not as extensive as the Los Alamos team. If and when testing becomes more extensive, demos could be arranged.
- Yes, we can demonstrate tamper detection of RF tags at 600 feet away. (No name or organization given.)
- We would consider product demonstrations in the future. (No name or organization given.)
- We would consider product demonstrations in the future (Scott H. Smith, Tyden-Brammall)
- Active seal demonstrations of capabilities.
- Yes, contact Susian Vickers, PM AIT for product demonstrations in AIT, RFID, Smart Card, and software programs.

6. While these Technical Symposiums were initially slanted toward mechanical and fiberoptic seals and Tamper-Indicating Devices, there has been more and more interest in RFID technology at these symposiums. We would appreciate your thoughts concerning the future focus of these Symposiums.

- This symposium was a perfect mix. ◆ Keep it broad. ◆ A mixture of all three.
- Would like presentations from users who will present how well the technology works, rather than from vendors alone.
- Include discussion on the use of RFID in worldwide deployment. Basically, what are the present problems and possible future solutions.
- In the DOE arena there is growing interest in active seal technologies which RFID technologies can be considered an intrinsic part.
- Any interest by attendees on secure pressure sensitive seal technologies?
- We should stay open to all new technologies.
- Yes, including other wireless (non-RF) technologies.
- Yes! RFID should be included in these symposiums.
- I still think the symposium should cover all of the relevant Tamper-Indicating Devices. There will hopefully always be new technologies that are not RF-based.
- Pressure-sensitive labels using holographic, prismatic, and laser-etching technology. 3M, NICOH, other vendors.
- I think that technology will move toward RF technology and it should be included in the symposium.
- I think future (next 2-3) symposiums should focus on users needs in terms of as-is; to-be focus on planning and moving into RFID.
- Let's go back to basics. There are: Passive seals, barrier seals, laser seals, active seals, and RFI — Do it all!

- Future symposiums should continue to focus on these aspects, as well as any emerging technology.
- The advance of the RFID technology makes it a vital element and should be a major focus in the future.
- Balance was good, but more emphasis on mechanical and fiberoptic would be good.
- Our needs are not so much for RFID. However, the electronic seals will, without a doubt, be used more in the future and discussion surrounding that is of benefit.
- RFID is going to be the future. It is important that this topic is covered.
- RFID is indeed important, but not the only seal available. The focus should remain on "all" types of seals industry. Mechanical, RFID, and other new technologies.
- I think the focus should be on new and emerging technology. However, don't forget to include any advances in the low tech sector.

7. **Do you have any comments concerning:**

Conference Facilities?

- Outstanding ◆ Excellent (9 comments) ◆ Great Facility (2 comments)
- Wonderful ◆ Very Good ◆ Good (2 comments) ◆ Fine ◆ OK (2 comments)
- No Problem!
- Very pleasant and conducive to a constructive meeting

Hotel Accommodations?

- Outstanding (3 comments) ◆ Excellent (8 comments) ◆ Great (2 comments)
- Very Good ◆ Good (2 comments) ◆ Fine ◆ OK (2 comments) ◆ No Problem!
- Very handy ◆ Excellent value
- The hotel is very pleasant with a wonderful location.
- Both were great. The lunches were also great, but possibly a choice would have been nice, even if only between two things. I'm not a vegetarian, but I feel bad for anyone who may have been. (Editor's Note: One vegetarian meal was served to an attendee as requested.)

7. **Did you like having the Symposium in the Channel Islands area?** Yes = 27 No=0. **Where else would you prefer to have the Symposium held?**

- Keep it here! ◆ Southern California. ◆ Florida, New Orleans (Gulf Coast).
- This place is great. ◆ Any easily accessible, self-contained hotel/conference center.
- San Diego, Seattle, San Francisco, Las Vegas.
- Florida, Washington, D.C. area (Policy Makers), locations near the overriding issues.
- This location is excellent, only alternative would be Washington, D.C.
- Not an issue for me. Can be anywhere.

AND COMMENTS FROM OUR DREAMERS . . .

- New Orleans, Hawaii, Bahamas, etc. ◆ Hawaii? No, seriously, this area is fine.
- Hawaiian Islands

8. Additional Comments?

- Consider spouses' program. ◆ Well done (2 comments). ◆ Excellent.
- Allow credit card payments. ◆ Job well done — Thanks.
- Good symposium but would have been interesting to hear from actual users of seals and their experiences.
- Make available speakers' notes and graphs to symposium participants.
- The Hanchett family did a great job of putting the symposium together and were very helpful.
- Great symposium. I was extremely pleased to be invited and look forward to working within this area.
- Good job, Bart! More publicity for conference. Make a poster.
- Need to make a concerted effort to have the owners and users of the Receipt, Stowage, Segregation, and Issue (RSSI) manual, TW0I0-AC-ORD-010 for the Navy to attend this conference.
- Very informative and helpful. Good work — Especially for Bart. Jane, Barbara, et. al.

4th DOD SECURITY SEAL SYMPOSIUM
✧ Listing of Attendees ✧

1325 15 July 1999

Darren Anderson
Chief Operating Officer
NIC Products
3100 Oak Road, Suite 210
Walnut Creek, CA 94596
925-930-2883 Fax: 925-930-2885
E-mail: <anderson@nicproducts.com>

Timothy (Tim) P. Besse
Security Consultant
CSSG/DoD
11600 Springfield Road
Laurel, MD 20708
301-210-1772 Fax: 301-210-1842
Home: 410-719-7297
E-mail: <Tbes1@aol.com>

William (Bill) Blasdell
Vice President, Engineering
SAVI Technology
450 National Avenue
Mountain View, CA 94043
650-934-8098 Fax: 650-428-0444
E-mail: <bblasdell@savi.com>

Randy Cabeen
Manager, Software Engineering and Testing and Verification Technology
TRW
6001 Indian School Road
Albuquerque, NM 87110
505-998-8227, Fax: 505-998-8115
E-mail: <randy.cabeen@trw.com>

Greg A. Chalfant
Program Control Analyst
Science Applications International Corp.
2109 Air Park Road, SE
Albuquerque, NM 87106
505-842-7813 Fax: 505-842-7760
E-mail: <greg.a.chalfant@cpmx.saic.com>

Van A. Collins
TID Administrator
Mason & Hanger Corporation - Pantex
PO Box 30030
Amarillo, TX 79120
806-477-4226 Fax: 806-477-3548
E-mail: <vcollins@pantex.com>

Tom Coyle
SAVI Technology
450 National Avenue
Mountain View, CA 94043
605-934-8192 Fax: 650-428-0444
E-mail: <tcoyle@savi.com>

James (Jim) C. Crabtree
Statistician
US Department of Energy
19901 Germantown Road
Germantown, MD 20874
301-903-6008 Fax: 301-903-8717
E-mail: <james.crabtree@hq.doe.gov>

Jerry Culpepper
Director of R&D
ProNet Tracking Systems
6340 LBJ Freeway
Dallas, TX 75240
972-687-2174 Fax: 774-0640

Kevin J. Curry
Federal Government Accounts Manager
3M Security Market Center
3M Center, Bldg 225-4N-14
St Paul, MN 55144-1000
St Paul Ofc: 651-733-3651
St Paul Fax: 651-737-8227
Wash DC Ofc: 202-331-6903
E-mail: <kjcurry@mmm.com>

Pat Duke
Lawrence Livermore National Lab
PO Box 808 (L-195)
Livermore, CA 94550
925-423-8441 Fax: 925-423-8441
E-mail: <duke1@llnl.gov>

Eric C. Elkins
Physical Security Specialist
Security Engineering Division, Code ESC-66
Naval Facilities Engineering Service Center
1100 - 23rd Avenue
Port Hueneme, CA 93043-4370
805-982-1567 Fax: 805-982-1253
E-mail: <elkinsec@nfesc.navy.mil>

4th DOD SECURITY SEAL SYMPOSIUM
✧ Listing of Attendees ✧

1325 15 July 1999

Steve Eynon
Stoffel Seals Corporation
400 High Avenue
Nyack, NY 10960
914-639-8593 Fax: 914-353-3876

Michael H. Farrar
Physical Security Specialist
Security Engineering Division, Code ESC-66
Naval Facilities Engineering Service Center
1100 - 23rd Avenue
Port Hueneme, CA 93043-4370
805-982-1574 Fax: 805-982-2444
E-mail: <farrarmh@nfesc.navy.mil>

Donald Ferguson
Vice President, Engineering
Kasten Chase
23 Oakdale Road
Maple, Ontario, Canada
905-238-6900 Fax: 905-238-6806
E-mail: <d.ferguson@kastenchase.com>

Simon Fiera
Technical Director
Encrypta Electronics Ltd.
Waterside Court, Albany Street, Newport, South Wales, NP9 5NT, UK
011-44-1633-859-859
Fax: 011-44-1633-859-755
E-mail: <sf@encrypta.com>

Anthony (Tony) R. E. Garcia
Senior Technician
Los Alamos National Laboratory
CST-1, MS J565
Los Alamos, NM 87545
505-667-6710 Fax: 505-665-4631
E-mail: <anthony@lanl.gov>

Bradley (Brad) P. Geno
Senior Security Specialist
STG, Inc./Department of State
11250 Waples Mill Road
South Tower, Suite 400
Fairfax, VA 22030
703-691-2480 Fax: 202–663-0304
E-mail: <genobr@hotmail.com>

Ronald (Ron) Wagoner Gilbert
Technical Group Manager
Pacific Northwest National Laboratory
PO Box 999
Richland, WA 99352
509-375-6672 Fax: 509-372-4725
E-mail: <ron.gilbert@pnl.gov>

Peter Kent Graham
President
Universeal USA, Inc.
105 San Felipe Way
Novato, CA 94945
415-898-4026, Fax: 415-898-4086
E-mail: <pkgraham@compuserve.com>

James R. Griggs
Program Coordinator
Pacific Northwest National Laboratory
3230 Q Street - PO Box 999
Richland, WA 99352
E-mail: <james.griggs@pnl.gov>

Barbara L. Hanchett
Owner/Manager
Farmers Insurance Agency
5740 Ralston Street, Suite 100
Ventura, CA 93003
805-654-0484 Fax: 805-658-9060
E-mail: <bberlin@aol.com>

Jane E. Hanchett
Director of Administration
Hanchett Engineering Associates
2585 Valley Meadow Ct., Suite B
Oak View, CA 93022-9513
805-649-4100 Fax: 805-649-1932
E-mail: <hanchett@jellink.net>

W. A. B. (Bart) Hanchett
Mechanical Design Engineer
Hanchett Engineering Associates
2585 Valley Meadow Ct., Suite B
Oak View, CA 93022-9513
805-649-4100 Fax: 805-649-1932
E-mail: <bart.hanchett@pnl.gov>

Mark Hayward
Sales and Marketing Director
Encrypta Electronics Ltd.
Waterside Court, Albany Street, Newport, South Wales, NP9 5NT, UK
011-44-1633-859-859
Fax: 011-44-1633-859-755
E-mail: <moh@encrypta.com>

Richard (Rick) Hellstrom
Engineer
Ricarl Design
1825 Roman Avenue
Camarillo, CA 93010
805-384-0645 Fax: 805-384-0745
E-mail: <hellstrom@iccas.com>

Robert (Bob) Herderhorst
Systems Engineer
Naval Undersea Warfare Center
610 Dowell Street
Keyport, WA 98345
360-396-1001 Fax: 360-396-1104
E-mail: <bherderh@kpt.nuwc.navy.mil>

Dave Hoegler
Systems Engineer - Code 712
Naval Surface Warfare Center - Earle
201 Hwy 34 South
Colts Neck, NJ 07722-5023
732-866-2859 Fax: 732-866-2805
E-mail: <dhoegler@noclant.navy.mil>

Patrick R. V. Horton
DOE/OSS Safeguards Seals Program Coordinator
Sandia National Laboratory
PO Box 5800 (MS 0759)
Albuquerque, NM 87185-0759
505-844-1044 Fax: 505-844-0011
Pager: 505-540-0016
E-mail: <prhorton@sandia.gov>

Fraser Jennings
SAVI Technology
450 National Avenue
Mountain View, CA 94043
650-934-8070 Fax: 650-428-0444
E-mail: <fjennings@savi.com>

Everett (Ev) Johnson
Deputy Director, Physical Security
Department of Defense
Ofc Asst Secretary of Defense (C^3I)
10340 Colony Park Drive
Fairfax, VA 22032
(703) 693-0290 Fax: (703) 614-9660
E-mail: <everett.johnson@osd.pentagon.mil>

Roger Johnston, PhD
Team Leader
Los Alamos National Laboratory
MS J565
Los Alamos, NM 87545
505-667-7414 Fax: 505-665-4631
E-mail: <rogerj@lanl.gov>

Jaime Lederer
Symposium Recorder
Naval Facilities Engineering Service Center
1100 - 23rd Avenue
Port Hueneme, CA 93043-4370
805-982-1694 Fax: 805-982-1594
E-mail: <ledererjd@nfesc.navy.mil>

Major Gregory (Greg) Louden
Defense Threat Reduction Agency
1680 Texas Street, SE
Kirtland AFB, NM 87117-5669
505-846-9615 Fax: 505-846-8611
E-mail: <loudeng@ao.dtra.mil>

Robert (Bob) W. Loughlin
Stanton Concepts
P.O. Box 139
Stanton, NJ 08885
908-236-7579 Fax: 908-236-7883
E-mail: <gigilough@aol.com>

Frank L. Lucero
Principal Technologist
Sandia National Laboratories
PO Box 5800 (MS-0815)
Albuquerque, NM 87185
505-844-2428 Fax: 505-284-4689
E-mail: <flucer@sandia.gov>

4th DOD SECURITY SEAL SYMPOSIUM
✧ Listing of Attendees ✧

1325 15 July 1999

Ralph J. Mallozzi
Stoffel Seals Corporation
400 High Avenue
Nyack, NY 10960
914-353-3800 X123 Fax: 914-353-3876
E-mail: <rmallozz@stoffel.com>

Odis McKinzie
Information Systems Analyst
Premier Technology Group
6551 Loisdale Court, Suite 990
Springfield, VA 22150
703-921-0090 Fax 703-921-0077
E-mail:
<odis.mckinzie@peostamis.belvoir.army.mil>

Jeffrey Miller
Mechanical Engineer
Security Engineering Division, Code ESC-66
Naval Facilities Engineering Service Center
1100 - 23rd Avenue
Port Hueneme, CA 93043-4370
805-982-1751 Fax: 805-982-1253
E-mail: <millerjd@nfesc.navy.mil>

James (Mitch) C. Mitchell
Department of State, PSD/CAT
2201 "C" Street NW, SA-14
Washington, DC 29522-0602
703-516-1513 Fax: 703-516-1503

James Najar
General Manager
ELC Security Products
530 Eleventh Ave.
San Diego, CA 92101
(619) 234-9203 or (800) 377-3257
Fax: (619) 234-0523
E-mail: <najar@elcsecurity.com>

Nazzari, Ian A.
Chief Executive Officer
NIC Products
3100 Oak Road, Suite 210
Walnut Creek, CA 94596
925-930-2883 Fax: 925-930-2885
E-mail: <iann@nicproducts.com>

Chris A. Pickett
Sensor Systems Group Leader
Lockheed-Martin Energy Systems
PO Box 2009
Oak Ridge TN 37831-8084
423-574-0891 Fax: (423) 576-2782
E-mail: <cap@ornl.gov>

Kim Rasmussen Hansen-Thybjerg
General Manager
ONESEAL, INC.
628 Route 10, #2
Whippany, NJ 07981
973-599-1155 Fax 973-599-1166
E-mail: <oneseal@onesealusa.com>

Eric D. Regaspi
Security Engineer
Department of State
2121 Virginia Avenue NW
Washington, DC 20037
703-235-0584, Fax: 703-235-0646
E-mail: <regaspie@state.gov>

Bruce C. Roberts
Encrypta Security Seals
3124 Hannah's Pond Lane
Oak Hill, VA 20171
703-620-9188 Fax: 703-620-9188
E-mail: <encrypta@aol.com>

Michael Ross
Senior Member of Technical Staff
Sandia National Laboratories
PO Box 5800 (MS-1371)
Albuquerque, NM 87185
505-844-3301 Fax: 505-284-5055
E-mail: <mpross@sandia.gov>

Ann M. Ruth
Scientist
Lawrence Livermore National Lab
7000 East Avenue
Livermore, CA 94550
925-423-6427 Fax: 925-424-5892
E-mail: <ruth1@llnl.gov>

Troy Shinn
Sales Manager
ELC Security Products
530 Eleventh Avenue
San Diego, CA 92101
619-234-9203 Fax 619-234-0523
E-mail: <troys@elcsecurity.com>

Rajiv Singh
Director, Business Development
EER Systems
10289 Aerospace Road
Seabrook, MD 20706-2280
301-306-7735 Fax: 301-306-7887
E-mail: <singhr@eer.com>

Scott Harrison Smith
Executive Vice President
Tyden-Brammall
409 Hoosier Drive
PO Box 208
Angola, IN 46703
713-662-3580 Fax: 713-662-3586
E-mail: <sharrisons@aol.com>

David (Dave) Straub
Member of Technical Staff
Sandia National Laboratories
PO Box 5800 (MS 1206)
Albuquerque, NM 87185
505-844-8651 Fax: 505-844-8784
E-mail: <dwstraub@sandia.gov>

Jennifer Elaine Tanner
Senior Research Scientist
Pacific Northwest National Laboratory
PO Box 999 (MS K3-55)
Richland, WA 99352
509-375-6626 Fax: 509-375-6936
E-mail: <jennifer.tanner@pnl.gov>

John Tichenor
Senior Staff Surveyor
CIGNA-MRMS
745 Garfield Avenue
Jersey City, NJ 07305
201-434-7498 Fax: 201-434-5971
E-mail: <john.tichenor@cigna.com>

Tobin Tanaka
Solicitor General - Canada
PO Box 9732, Station "T"
Ottawa, Ontario, K1G 4G4, Canada
613-842-1853 Fax: 613-842-1841

Lynn Torres
Assistant Program Manager, USMC Programs
Naval Facilities Engineering Service Center
1100 - 23rd Avenue
Port Hueneme, CA 93043-4370
805-982-1388 Fax: 805-982-1458
E-mail: <torreslm@nfesc.navy.mil>

Susian E. Vickers
Product Manager, US Army
PEO STAMIS (attn: SFAE-PS-AIT)
Automatic Identification Technology
9350 Hall Road, Suite 142
Fort Belvoir, VA 22060-5526
DSN: 656-4110
703-806-4110 Fax: 703-806-3214
E-mail:
<susian.vickers@peostamis.belvoir.army.mil>

Captain Robert J. Westberg, Jr.
Commanding Officer
Naval Facilities Engineering Service Center
Code-00
1100 - 23rd Avenue
Port Hueneme, CA 93043-4370
805-982-1393 Fax: 805-982-4429
E-mail: <westbergrj@nfesc.navy.mil>

Richard F. Williams, CPP
Director of Security
Office of the Deputy Assistant Secretary of
Defense (Security & Information Operations)
The Pentagon,
Washington, DC 20301
(703) 614-0578 Fax: (703) 614-9660
E-mail: <Richard.Williams@osd.pentagon.mil>

Christopher W. Wilson
Senior Member, Technical Staff
Sandia National Laboratories
PO Box 5800, MS 1003
Albuquerque, NM 87185
505-844-5888 Fax: 505-844-6161
E-mail: <cwwilso@sandia.gov>

Eric John Wood
Major Account Executive
ProNet Tracking Systems
6340 LBJ Freeway
Dallas, TX 75240
972-687-2187 Fax: 972-774-0640
E-mail: <ewood@pronettracking.com>